Der Hamburgische Datenschutzbeauftragte

Microsoft Backoffice unter NT-Server 4.0

– eine datenschutzorientierte Analyse

O. Höwer
Oktober 1998

MS BackOffice

- Eine datenschutzorientierte Analyse

1. Windows NT Server 4.0. 3

2. Microsoft BackOffice. 5

2.1 SQL Server 6.5 5

2.2 SMS 1.2. 10

2.3 Exchange Server 5.5. 14

2.4 SNA Server 4.0. 20

2.5 Proxy Server 2.0 23

2.6 Internet Information Server 26

2.7 Index Server 31

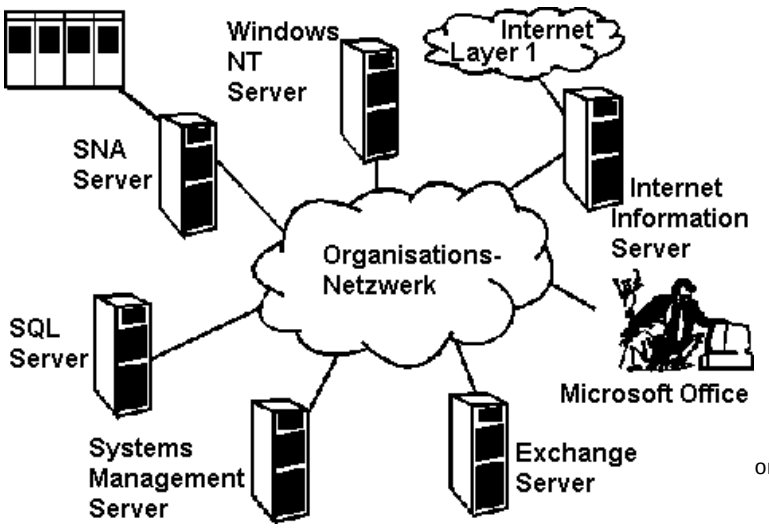
2.8 Andere Komponenten. 33

Anhang

Abkürzungsverzeichnis. 34

Abbildungsverzeichnis. 35

Literatur. 36



omponenten von Microsoft BackOffice

Vorwort

Diese Ausarbeitung richtet sich an all jene, die eines oder mehrere der BackOffice-Produkte aus dem Hause Microsoft einsetzen bzw. deren Einsatz planen. Sie setzt sich zum Ziel, einen Beitag zur Sicherung der betroffenen Netze und der in ihnen gespeicherten personenbezogenen Daten zu liefern. Insbesondere spricht das vorliegende Papier Datenschutzbeauftragte aus dem öffentlichen und nicht-öffentlichen Bereich sowie Systemadministratoren an.

Zunächst wird ein allgemeiner Überblick über die einzelnen Komponenten von MS BackOffice und deren Funktionsumfang gegeben, anschließend werden die für einen sicheren Betrieb relevanten Aspekte erläutert. Auf Windows NT Server wird nur oberflächlich eingegangen, da zu diesem Produkt bereits diverse Sicherheitsanalysen vorliegen. Zum Abschluß jedes Abschnitts werden zusammenfassende Handlungsempfehlungen für einen sicheren Betrieb des Produktes erteilt.

1. Windows NT Server

1.1 Funktionsbeschreibung

Microsofts Windows NT Server wurde als multifunktionelles Serverbetriebssystem entwickelt, das sowohl gute Geschwindigkeit als Datei- und Druckerserver als auch entsprechende Leistungsfähigkeit als Applikationsserver bietet. Es ist ein sehr einfach zu bedienendes Netzwerkbetriebssystem mit hoher Robustheit und Skalierbarkeit für kritische Anwendungen.

Zum Lieferumfang gehört darüber hinaus der Microsoft Internet Information Server (IIS), ein Web-Server, der auf Windows NT 4.0 aufsetzt. Die gegenüber NT 3.51 vorgenommenen Änderungen erlauben die Verwendung von Domain-Namen für Verbindungen zwischen Server und Arbeitsstationen über das Internet. Weiterhin können DNS-Server auch entfernt administriert werden können. Windows NT Server bietet Wählzugriff über den Remote Access Service (RAS). Eine Workstation stellt mit der RAS-Client-Software eine Client-Sitzung her.

Darüber hinaus ist im Windows NT Server 4.0 der Multi-Protocol Router (MPR) integriert. Dieser Service ermöglicht es, Windows NT Server auch als Router für LAN-Verbindungen, z.B. über X.25 oder ISDN, zu verwenden. Der Routing Service arbeitet mit den Protokollen IPX/SPX, TCP/IP und Appletalk.

Der Windows NT Server ist zudem die Plattform für Email-Systeme (Exchange Server), Dateiserver, Datenbanken, Internet- und Kommunikationsdienste, die z.B. durch Microsoft BackOffice-Produkte impementiert werden können. Da Microsoft BackOffice über eine offene Architektur verfügt, läßt es sich in bestehende Systeme, z.B. NetWare-, UNIX- und Großrechnerplattformen, integrieren.

Wesentliche Funktionen des NT Servers sind:

- NetWare Dienste
- TCP/IP-Dienste
- Remote Access Service RAS
- EventLog Service (Protokollierung)
- NTFS Sicherheitsfunktionen
- Host Zugang mit Zusatzprodukt SNA möglich
- Unterstützung von Skripts
- Revision

1.2 Sicherheitsaspekte

Sicherheit bieten in erster Linie ein Domänenkonzept sowie mit individuellen Berechtigungen versehene Benutzerkonten. Große Benutzerzahlen können durch Erteilen von Berechtigungen für Gruppen und Hinzufügen von Benutzern zu Gruppen verwaltet werden.

Dieses Sicherheitssystem funktioniert über einen Verbund von Domänen-Controllern. Durch diese Verteilung werden sowohl Skalierbarkeit als auch Verfügbarkeit erreicht. Einzelne Domänen können über 40.000 Benutzer aufnehmen. Die NT-Sicherheit geht über diese Zahl hinaus, indem sie sich über eine Architektur mit mehreren Domänen erstreckt, in der Vertrauensstellungen zwischen den einzelnen Domänen bestehen.

Das Sicherheitssystem weist sowohl eine programmtechnische als auch eine intuitive grafische Benutzerschnittstelle auf, die für jeden Knoten die Verwaltung der Netzwerksicherheit ermöglicht. Sicherheitstechnisch bedenklich ist die Tatsache, daß die Kommunikation zwischen Windows-NT-Rechnern über die Netbios-Ports 137,138 (UDP) und 139 (TCP) sowie einen dynamischen Port (> 1024) erfolgt, so daß sämtliche Ports in diesem Bereich erreichbar sein müssen. Dieses Verhalten bringt u.U. umfassende Sicherheitsmängel mit sich, da für jeden außerhalb des Netzes befindlichen Angreifer die offenen Ports erkennbar sind und einem Angriff z.B. durch Erraten von Paßwörtern nichts im Wege steht. Insbesondere für das Administrator-Paßwort ist daher eine sichere Wahl zu treffen, d.h. eine Kombination aus Groß-/Kleinschreibung, Ziffern und Sonderzeichen sollte Vorschrift sein. Abhilfe kann u.U. auch eine Konstellation schaffen, in der die Server zur externen Kommunikation zu einem physikalisch getrennten Netz zusammengefaßt werden, das eine eigene Domäne bildet. Zu den Domänen der einzelnen Abteilungen der Organisation werden von hier einseitige Vertrauensbeziehungen eingerichtet, so daß zwar ein Zugriff auf die Kommunikations-Server ermöglicht, ein Durchgriff auf andere Domänen jedoch verhindert wird.

Windows NT Server verwendet Sicherheit auf Benutzerebene. Das bedeutet, daß mit jedem Konto eine Liste mit Genehmigungen assoziiert wird. Die gemeinsame Ressourcenverwendung in Windows for Workgroups 3.11 und Windows 95 verwendet im Vergleich dazu Sicherheit auf Ressourcenebene – Genehmigungen werden mit jeder gemeinsam verwendeten Ressource assoziiert.

Windows NT schützt jede gemeinsam verwendete Ressource im System. Wenn sich ein Benutzer anmeldet, erstellt Windows NT ein Zugriffs-Kurzzeichen für diesen Benutzer, das den Benutzer und alle Gruppen, denen der Benutzer angehört, identifiziert. Windows NT überprüft das Kurzzeichen jedesmal, wenn der Benutzer (oder eine Programmgruppe unter dem Benutzerkonto) Zugriff auf eine Systemressource fordert. Windows NTs Security Reference Monitor (SRM) analysiert Benutzer- und Gruppengenehmigungen für das Objekt und trifft eine Entscheidung. Es bestehen bzgl. der grundlegenden Sicherheitsmechanismen keine Unterschiede zwischen dem NT-Server und einer -NTWorkstation.

Der EventLog Service bietet eine einfache Methode zum Erfassen von Informationen über den System-Start, Konfigurationsfehler, Sicherheitsereignisse und Anwendungsereignisse. Diese Informationen sind die wichtigste Quelle für Fehlerbehebung und die Leistungsüberwachung.

Windows NT Server kann Erfolg und Mißerfolg für jedes der folgenden Sicherheitsvorkommnisse protokollieren:

- Anmelden und abmelden.
- Benutzer- und Gruppenverwaltung.
- Prozeßaufzeichnung.
- Datei- und Objektzugriff.
- Neustart, ausschalten & Systemsicherheit

Windows NT Server zeichnet folgende Ereignisse in seinen drei Protokolldateien auf:

- Systemprotokoll. Aufzeichnen von Systemereignissen
- Sicherheitsprotokoll. Zeichnet Ereignisse für Revisionen auf.
- Anwendungsprotokoll. Für Anwendungen zum Aufzeichnen wichtiger Ereignisse.

Die Protokolle zeichnen fünf verschiedene Ereignistypen auf:

Informationsereignisse, Warnereignisse, Kritische Fehler, Erfolgs- und Mißerfolgsrevisionen.

Für eine genauere Analyse des Windows NT Basissystems und seiner Sicherheitsvorkehrungen vergleiche z.B.: Groß, Alfred - *Analyse der Sicherheitsfunktionalitäten des Netzwerkbetriebssystems Windows NT*, Der Hamburgische Datenschutzbeauftragte, Dezember 1996.

2. Microsoft BackOffice

2.1 SQL-Server

2.1.1 Funktionsbeschreibung

Microsoft SQL Server ist ein relationales Datenbank-Managementsystem, das den im unteren Leistungsspektrum notwendigen Umfang abdeckt. Er ist eine Ergänzung der Intranet- und Internet-Serverstruktur um eine Datenbank, in der man alle relevanten Daten speichern, aufbereiten und abrufen kann. Dieses Datenbankmanagementsystem nutzt die Prinzipien der Client-Server-Datenverarbeitung. Als Clients können z.B. der SQL Enterprise Manager, MS Access aber auch jede andere Clientsoftware, die eine ODBC- oder DB-Library-Schnittstelle besitzt, eingesetzt werden.

Zu den Eigenschaften des RDBMS gehören die Transaktionsverarbeitung, die Aufrechterhaltung der Referenzdatenintegrität, die Transaktionsverteilung sowie die Datenreproduktion bzw. integrierte Datenreplikation. Es verfügt außerdem über einen Satz vollgrafischer Verwaltungshilfsmittel. Durch die Skalierbarkeit von Windows NT ist der SQL Server an verschiedene Unternehmensgrößen und Aufgaben einfach adaptierbar. Das BackOffice-Paket 2.0 enthält noch den SQL Server 6.0. Microsoft SQL Server 6.5 wurde erst kurz nach Herausgabe von BackOffice 2.0 auf den Markt gebracht.

Auffallend sind die zwingenden Abhängigkeiten anderer MS Backoffice-Produkte vom SQL-Server. Letzterer verfügt über eine eingebaute Integration mit dem Microsoft Internet Information Server. Weiterhin ist auch der Systems Management Server (SMS) nicht ohne eine Installation des SQL Servers zu betreiben. SMS speichert die Informationen über das Netzwerk in einer SQL Server-Datenbank. Dadurch wird die Zeit reduziert, die notwendig ist, um SMS zu verwalten, weil die Datenbankverwaltung bereits als Teil der SQL Server-Installation durchgeführt wird. Der Exchange Server stützt sich hingegen noch nicht auf den SQL-Server, sondern auf eine interne Microsoft-Datenbank. Die starke Integration in Windows NT Server und die BackOffice-Familie wurde in Release 6.5 konsequent fortgesetzt und spiegelt sich z.B. in der Unterstützung des Exchange Servers 5.0 wieder. Microsoft wird auch in der Zukunft dieses Muster für seine BackOffice- Produkte beibehalten.

Zu den wichtigsten Erweiterungen und Neuerungen in Version 6.5 zählen die Integration des Transaktionskoordinators DTC (Distributed Transaction Coordinator), die Unterstützung für das Internet, neue Funktionalitäten für den Einsatz als Data Warehouse-Datenbank sowie die Unterstützung der PowerPC-Plattform. Verteilte Transaktionen über mehrere voneinander unabhängige Datenbankserver können im neuen Release sehr einfach mit dem Distributed Transaction Coordinator (DTC) realisiert werden. Dieser neue unter Windows NT laufende Service ermöglicht auch die Verteilung von Transaktionen mittels anderer Transaktionsmonitore im Unternehmensnetzwerk. Neben den Standards, die bereits die Vorgängerversion erfüllte (wie ODBC, OLE, MAPI und Win32), beinhaltet die neue Version nun auch den ANSI-92 Standard, SNMP, XA und ist als eine von wenigen relationalen Datenbanken NIST- und FIPS-zertifiziert. Weiterhin unterstützt der SQL-Server die standardisierten Netzwerkprotokolle TCP/IP, IPX/SPX, NetBEUI, DEC Pathworks, Apple Talk, Vines IP und SNA (über den Microsoft SNA Server). Um den Microsoft SQL Server auch als Datenbank im Data Warehouse einsetzen zu können, wurde neben dem CUBE- und dem ROLLUP-Operator eine Replikation zu heterogenen Datenbanken (z. B. Oracle, Sybase oder auch Microsoft Access) in das Produkt implementiert.

Die Struktur der Datenbank kann mit dem SQL Server flexibel mit grafischen Tools aufgebaut und verwaltet werden, wobei man die Daten beliebig im Netzwerk verteilen kann. Die gesamte Administration läßt sich von einer Arbeitsstation aus steuern. Durch die Kompatibilität der einzelnen BackOffice Produkte paßt der SQL Server in die Struktur des NT Servers und somit auch als Ergänzung zum Internet Information Server, woraus sich gute Voraussetzungen für eine Internet-Präsentation von Daten ergeben. Die Darstellung der Datenbankin-

halte kann man mit dem Web Assistenten an die gewünschten Vorlagen einspielen. Dies erlaubt eine benutzerfreundliche Darstellung der abgerufenen Dateninformationen. Die Performance und der schnelle und gesicherte Informationszugriff wird dabei kaum beeinträchtigt. Dabei spielt es nur eine geringe Rolle, welches Datenvolumen man über den SQL Server generiert.

Von besonderer praktischer Bedeutung sind:

- Integration von Microsoft Office- und BackOffice-Anwendungen
- Niedrige Betriebskosten - das heißt, geringer Bedarf an technischer Unterstützung, kurze Entwicklungszeiten und niedrigere Hardware/Softwareausgaben
- Unterstützung von Standard-SMP-Hardware (SMP: Symetric Multiprocessing) - bietet effiziente Skalierbarkeit
- Offene Standards - Unterstützung von ODBC, SNMP, ANSI-SQL, HTML, Java und alle gängigen Netzwerkprotokolle
- Verwaltungswerkzeuge für eine einfache und zentralisierte Verwaltung
- Integration in Internet und Intranet - der Web-Assistent erzeugt auf Grundlage von Daten aus SQL-Server nach Zeitplan oder über Trigger gesteuert HTML-Seiten

2.1.2 Sicherheitsaspekte

Zugriffsrechte

Die Sicherheit des SQL-Servers umfaßt verknüpfte Elemente (Tabellen, Sichten, gespeicherte Prozeduren), anhand derer diverse Beschränkungen festgelegt werden können. Im einzelnen läßt sich bestimmen, welche Benutzer sich anmelden können, wer auf eine bestimmte Datenbank zugreifen darf, auf welche Datenbankobjekte ein Benutzer zugreifen darf und welche Transact-SQL-Anweisungen ein Benutzer auf den verschiedenen Datenbanken, auf die er Zugriff hat, ausführen darf. Man kann sehr flexibel festlegen, wer in den Tabellen oder Sichten der Datenbanken oder sogar in einzelnen Spalten Daten einsehen oder ändern kann.

Die SQL-Sicherheit baut dabei auf den Sicherheitsmechanismen des Windows NT-Servers auf (Abb.2).

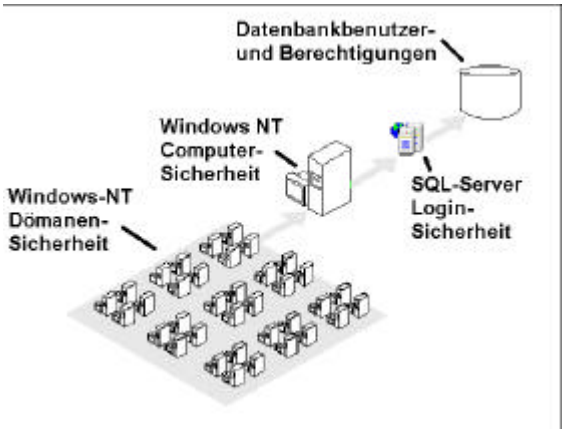


Abb.2: Sicherheitshierarchie

Es kann auch ein automatisiertes System erstellt werden, das Gruppen einrichtet und Berechtigungen zuweist; als Grundlage hierfür dienen Abfrageergebnisse aus anderen Anwendungen oder bestimmte
Daten, beispielsweise Organigramme oder Listen mit Mitarbeiterpositionen. Um eine Anwendung zu erstellen, die Sicherheitsmaßnahmen für ein Datenbanksystem einrichtet, kann VB Datei-E/A, OLE oder API verwendet werden. Die Informationen können im Anschluß verwendet werden, um Login-, User- oder Group- Objekte zu erstellen. Anschließend werden mit Hilfe der Methode *Grant* Berechtigungen für Table-, Database- oder StoredProcedure-Objekte zugewiesen. Das unbefugte Einschleusen solch automatisierter Programme mit dem Ziel, sie später vom ‚Super-User' unwissentlich ausführen zu lassen, kann durch sehr restriktive Handhabung der NT-basierten Zugriffsberechtigungen verhindert werden.

Authentisierung

Der SQL-Server bietet System- und Datenbankadministratoren die Möglichkeit festzulegen, welchen Clients eine Anmeldung beim Server erlaubt ist. Er verfügt hierfür über 3 Sicherheitsmodi, die wie die meisten Sicherheitsoptionen im SQL-Enterprise Manager festgelegt werden:

1. ***Standard-Sicherheit***: Dieser Modus ist standartmäßig voreingestellt. Bei jeder Verbindungsanfrage wird ein Client zusätzlich zum vorher erfolgten Windows-NT Login zur Angabe eines Benutzernamens und Kennwortes aufgefordert. Hierbei setzt SQL Server sein eigenes Authentisierungsverfahren für alle Verbindungen ein (außer wenn Clientanwendungen ausdrücklich die integrierte Sicherheit über die vertrauten Verbindungen anfordern).
2. ***Integrierte Sicherheit***: Der SQL-Server erhält die Anmeldeinformationen vom NT-Sicherheitssystem, so daß keine zusätzlichen Anmeldungen erforderlich sind. Eine Verbindung, die von einem Client in diesem Modus hergestellt wird, wird als vertraute Verbindung bezeichnet. Beim integrierten Modus werden für alle Verbindungen Windows NT-basierte Echtheitsbestätigungsverfahren eingesetzt. Nur vertraute Verbindungen mit dem SQL Server sind zulässig. Der in der Login-Anforderung von einer DB-Library- oder ODBC-Clientanwendung (Open DataBase Connectivity) angegebene Login-Name und das SQL Server-Kennwort werden von SQL Server ignoriert. Netzwerkbenutzer, denen Berechtigungen auf Benutzerebene für SQL Server erteilt wurden, melden sich unter ihrem Netzwerkbenutzernamen bzw. der Standard-Login-ID an (falls der Netzwerkbenutzername nicht in der Tabelle *syslogins* gefunden wird).
3. ***Gemischte Sicherheit***: Der SQL-Server ermöglicht auch eine Kombination aus integriertem und Standard-Modus. Hierbei sind sowohl vertraute als auch nichtvertraute Verbindungen zulässig. Bei vertrauten (Multi-Protokoll- oder Named Pipes-) Verbindungen untersucht SQL Server den angegebenen Login-Namen in der Form, wie er von der Client-DB-Library- oder ODBC-Anwendung angegeben wurde. Stimmt der Login-Name mit dem Netzwerkbenutzernamen des Benutzers überein oder wird keine Benutzerkennung eingegeben, versucht SQL Server zunächst, wie oben beschrieben, die Anmelderegeln des integrierten Modus anzuwenden. Schlägt dies fehl, verwendet SQL Server die Standardregeln.

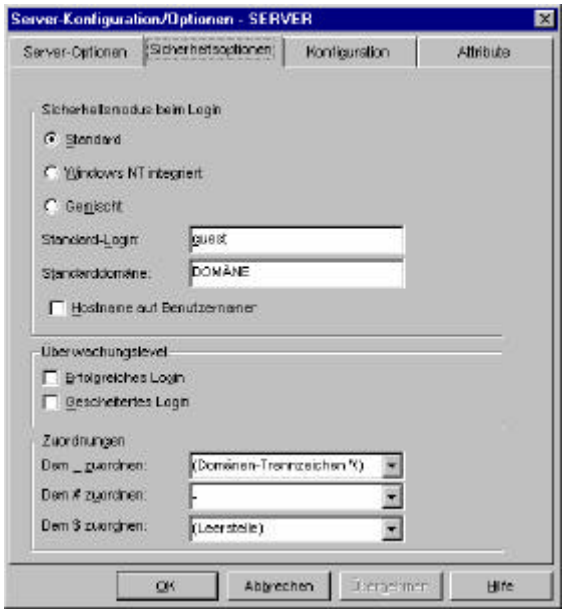


Abb.3: SQL-Sicherheitsmodi

Weitere Informationen zu den Sicherheitsmodi finden sich im Benutzerhandbuch sowie in der Online-Dokumentation im Systemadministratorhandbuch, Teil 4 (Sicherheit), Kapitel 8 (Sicherheitskonzepte), „Sicherheitsmodus des Servers beim Login“.

Zugriffsschutz

Die Anweisungen zur Datenmanipulation (Einfügen, Aktualisieren, Löschen) sind mit Hilfe einer gespeicherten Prozedur zu verwalten, so daß es dem Benutzer nicht ermöglicht wird, die Tabellendaten direkt zu manipulieren.

Die Anweisungen können zwar direkt ausgeführt werden, aber das Einschließen in gespeicherte Prozeduren bietet zusätzliche Sicherheit und Wartungsfreundlichkeit. Gespeicherte Prozeduren bieten höchst wirksame Methoden zur Sicherung der Datenintegrität in gemischten Anwendungsumgebungen. So kann beispielsweise verhindert werden, daß Benutzer o.g. UPDATE, INSERT- und DELETE-Operationen außerplanmäßig auf Tabellen vornehmen. Der Systemadministrator kann genau kontrollieren, wann und auf welche Weise Daten für die einzelnen Benutzer oder Benutzergruppen in der Datenbank geändert werden.

Der SQL-Server unterstützt die sog. WITH CHECK OPTION auf Sichten, wodurch sichergestellt werden kann, daß Benutzer nur die Daten abfragen und ändern können, die ihnen durch die Sicht angezeigt werden. Diese Option gewährleistet, daß alle an der Sicht durch-

SQL Enterprise Manager
Einstellen der Login-Sicherheit
Benutzer-Manager
Erstellen von Windows NT-Benutzern und -Gruppen
SQL Security Manager
Erteilen der Zugriffsberechtigung auf SQL Server für Windows NT-Benutzer und Gruppen
SQL Enterprise Manager
Einstellen von Objektberechtigungen für jede Datenbank
SQL Enterprise Manager
Einstellen von Anweisungsberechtigungen für jede Datenbank
Abb.4: Hierarchie der SQL-Sicherheitseinstellungen

geführten Anweisungen zur Datenänderung die Kriterien erfüllen, die in der für die Definition der Sicht verwendeten SELECT-Anweisung festgelegt wurden.

Verschlüsselung

Die Multi-Protokoll-Net-Library unterstützt die Verschlüsselung von Daten, insbesondere Paßwörtern, bei der Kommunikation über vertraute Verbindungen. Die Verschlüsselung kann entweder auf dem Client eingestellt oder vom Server für alle Clients erzwungen werden. Bei der vom Server erzwungenen Verschlüsselung wird automatisch die gesamte Kommunikation zwischen Client, der die clientseitige Multi-Protokoll-Net-Library verwendet, und dem Server, der die serverseitige Multi-Protokoll-Net-Library verwendet, verschlüsselt.

Die vom Server erzwungene Verschlüsselung wird nur von der Multi-Protokoll-Net-Library unterstützt. Falls daneben auf dem Server Net-Libraries für andere Protokolle geladen werden, verwenden eingehende Verbindungen über diese Net-Libraries keine Verschlüsselung. Das Net-Library-Multi-Protokoll nutzt die Vorteile der abgesetzten Prozeduraufrufe (RPC) von Windows NT. Im Gegensatz zu anderen Net-Libraries muß die Multi-Protokoll-Net-Library lediglich als Option in dem Dialogfeld Auswahl der Netzwerkprotokolle gewählt werden und erfordert keine Eingabe von Konfigurationsparametern. Darüber hinaus erfüllt die Multi-Protokoll-Net-Library folgende Funktionen:

- Kommunikation über die meisten von Windows NT unterstützten IPC-Mechanismen.
- Verwendung der integrierten Sicherheitsfunktionen, die RPC unterstützt (einschließlich Novell-Clients unter Windows, die SPX oder IPXODI verwenden).

Der SQL-Server bietet nur sehr eingeschränkte Möglichkeiten zur Verschlüsselung von Daten aud dem Datenträger. Allenfalls gespeicherte Prozeduren, Sichtdefinitionen oder Trigger können mit Hilfe der Klausel WITH ENCRYPTION in der Tabelle *syscomments* verschlüsselt und so vor dem Benutzer verborgen werden, sofern dies unbedingt notwendig ist.

Administration

Der Datenbankadministrator (DBA) installiert den Microsoft SQL Server, erstellt Verfahren und Standards, plant die Kapazitätsanforderungen und ggf. Datenbanken und Server-Prozesse, sichert und korrigiert ggf. Datenbanken, verbessert die Leistung der Datenbankanwendungen, hilft Anwendungsentwicklern und Datenbankverwendern bei sämtlichen Datenbankproblemen. Ein DBA kann auch für die Verwaltung der Daten verantwortlich sein, die in den SQL Server-Datenbanken der Organisation gespeichert sind.

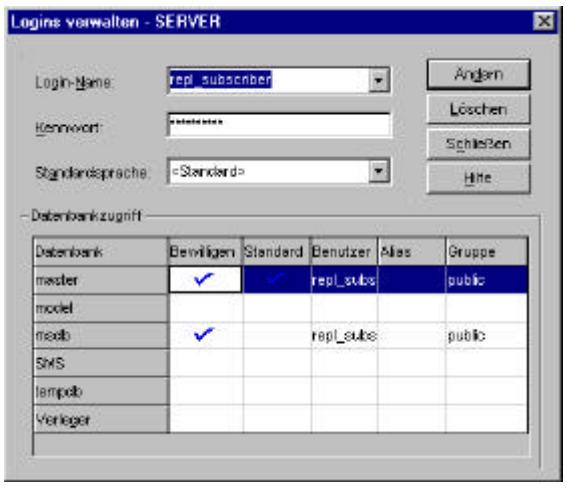


Abb.5: Rechtevergabe im SQL-Enterprise-Manager

Bei derart umfassenden Möglichkeiten sollte bei der Definition der Rechte besonders sorgfältig vorgegangen werden. Da die Rechtedefinition sich auch auf abhängige Programme auswirken kann (z.B. SMS), sollten allzu weitreichende Kompetenzen (insb. die Rechtevergabe selbst) nicht in die Hände eines einzelnen gelegt werden.

Da ein Zugang nach dem Vier-Augen-Prinzip vom System selbst nicht vorgesehen ist, bietet sich die Einrichtung eines geteilten ‚Super-User'-Passworts für mehrere Administratoren an. Jeder einzelne erhält ansonsten spezialisierte Rechte für den jeweils zugedachten Verantwortungsbereich. Es bietet sich an, zumindest die Berechtigungen des Datenbankadministrators und des Netzwerkadministrators zu trennen. Der Datenbankadministrator sollte be-

züglich der SMS- und anderer Login-Datenbanken eingeschränkte Rechte erhalten, so daß eine Manipulation der Kompetenzen weitgehend ausgeschlossen wird. Im übrigen können auch Benutzer oder ganze Benutzergruppen, die zuvor im Windows NT-Benutzer-Manager eingerichtet worden sind, zur Verwendung unter SQL-Server eingerichtet werden. Als Hilfsmittel zur Autorisierung dieser Gruppen dient der SQL-Security Manager:

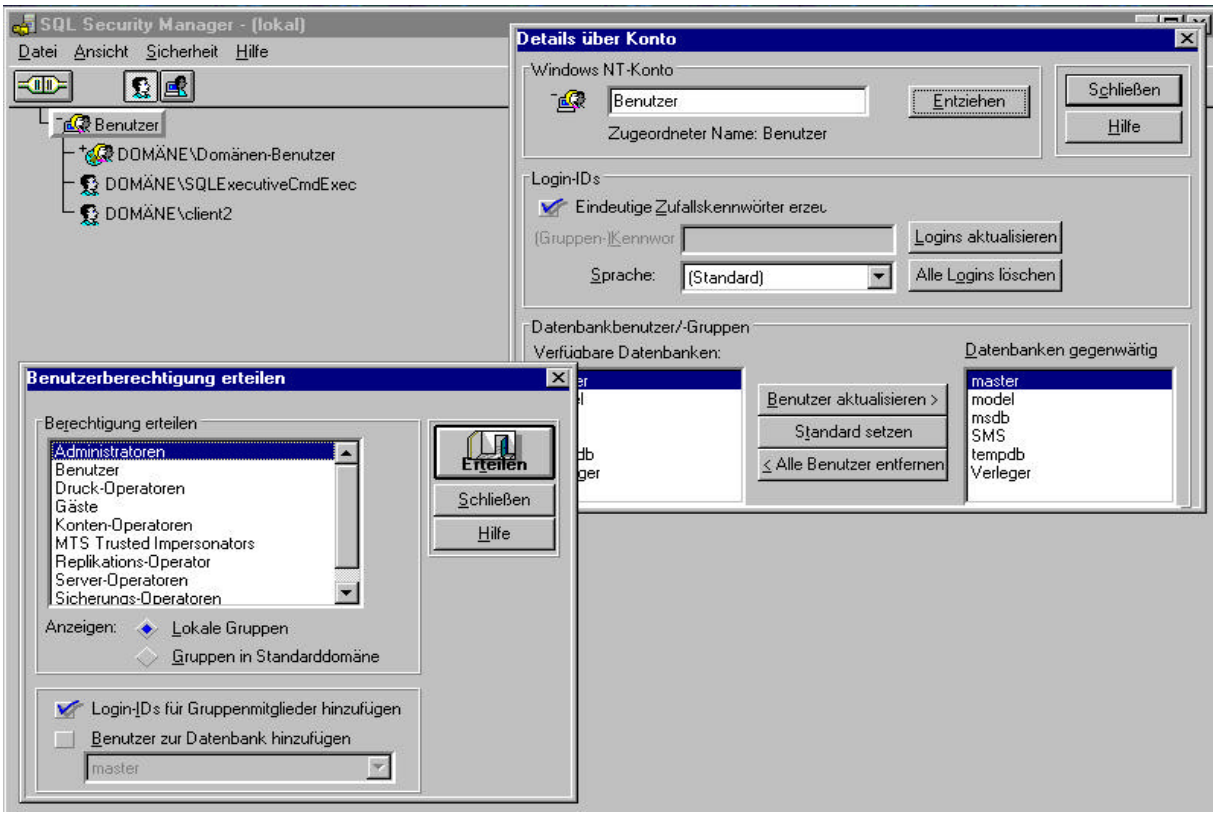


Abb.6: Der SQL-Security-Manager

Einzelaspekte

Vorsicht ist geboten, wenn neben dem SQL-Server auch der IIS installiert ist. Wird der Web-Server über das ‚NT-Option Pack' eingerichtet, installiert sich standardmäßig der Remote Data Service (RDS) für den Datenbankzugriff über das Web. Dieser widerum enthält einen Bug, der Eindringlingen Zugang zu sämtlichen Daten der Organisation bietet. Das Risiko des unerlaubten Zugriffs steigt, wenn OLE-DB-Provider installiert sind. Sie erlauben zusätzlich die Ausführung von Shell-Kommandos. Der RDS-Dienst ist also unbedingt zu deaktivieren.

Handlungsempfehlungen:

- Das Prinzip der minimalen Zugriffsrechte muß Anwendung finden, d.h. Benutzer und Operatoren dürfen nur die Rechte erhalten, die sie zum Ausüben Ihrer Tätigkeit benötigen.
- Sollen die Zugriffsberechtigungen automatisiert zugewiesen werden (z.B. mit der Methode *Grant* oder dem Security Manager auf Basis der NT-Zugriffsrechte), sollte unbedingt eine Nachbesserung und Pflege der Rechte gemäß des oben genannten Punktes erfolgen.
- Anweisungen zur Datenmanipulation dürfen ausschließlich über gespeicherte Prozeduren erfolgen.
- Die Multi-Protokoll-Net-Libary sollte verwendet werden, um anschließend von Seite des Servers eine Verbindungsverschlüsselung für alle Clients zu erzwingen.
- Administrationsrechte, die über die zum Tagesgeschäft notwendigen hinausgehen, sollten mit einem zusammengesetzten ‚Super-User'-Passwort nach dem Vier-Augen-Prinzip geschützt werden, so daß eine Autorisierung von mindestens zwei Administratoren erfolgt.
- Besondere Sorgfalt sollte bei der Installation des SQL-Server auf die Auswahl des geeigneten Sicherheitsmodus gelegt werden. Eine allgemeine Empfehlung diesbezüglich läßt sich nicht geben, da die individuelle Nutzung hierfür ausschlaggebend ist. In vielen Fällen reiner geschlossener Windows-NT Netze ist integrierte Sicherheit sicherlich ausreichend.

• Wenn es die Organisationsstruktur zuläßt , sollte der NT-Administrator nicht gleichzeitig DBA sein.
• Der RDS (Remote Data Service) des IIS muß unbedingt deaktiviert werden.

2.2 Systems Management Server

2.2.1 Funktionsbeschreibung

Microsoft Systems Management Server wurde für die Verwaltung von vernetzten PC‘s entwickelt. Er fügt sich dabei nahtlos in die bereits vorhandene Systemumgebung durch die Unterstützung der gängigen Netzwerkmanagementsysteme wie etwa HP OpenView, CA Unicenter oder SNI TransView ein. Der Systems Management Server ermöglicht die Verwaltung räumlich verteilter Windows-basierter Rechner von einer zentralen Stelle aus. Durch seine Architektur kann man in Netzen jeder Größenordnung, die aus diversen Domänen bestehen können, typischerweise jedoch auf einen Standort beschränkt bleiben, alle Aufgaben einer zentralen PC-Administration erledigen.

Um die installierten Anwendungen zu inventarisieren, erkennt der SMS Inventory Agent bis zu 4500 Standardapplikationen. Dies versetzt den Administrator in die Lage, auf einfache Weise zu kontrollieren, welche Anwendungen tatsächlich installiert sind und wie viele Kopien davon im Netzwerk vorhanden sind. Weiterhin lassen sich die Rechner innerhalb des Netzwerks problemlos lokalisieren, Hardware-Konfigurationen erfassen und Schlüsselinformationen zurück an eine zentrale Datenbank senden, auf der sämtliche Bestandsdaten des SMS gespeichert werden. Mit Hilfe dieser Informationen hat man die Möglichkeit, die Verteilung von neuen Anwendungsprogrammen und Update-Versionen effizient zu planen. SMS erlaubt die automatische Verteilung und Installation sämtlicher Software von zentraler Stelle aus.

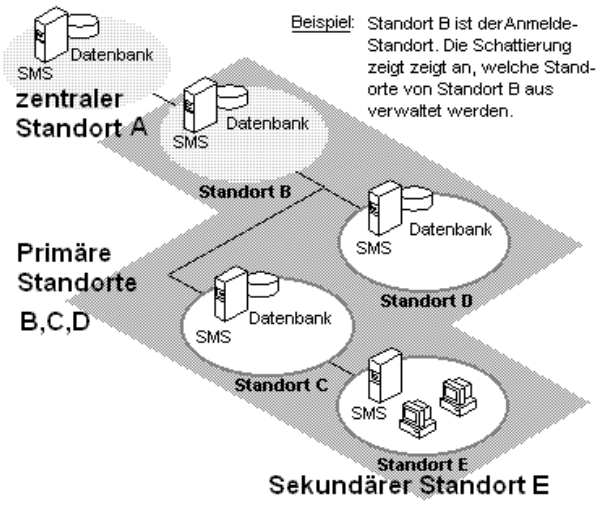


Abb.7: Beispiel einer SMS-Standorthierarchie

Jeder primäre Standort muß über eine eigene Standort-Datenbank verfügen.

Darüber hinaus lassen sich beliebig viele sekundäre Standorte einrichten, die ihre Bestandsdaten an den übergeordneten primären Standort weiterleiten. Ausgehend von einem zentralen Standort, der Wurzel eines Hierarchiebaumes, läßt sich so eine beliebige Struktur von Standorten erstellen.

Die Remote-Control-Funktion ermöglicht einem Systemadministrator, jede Operation auf einer Windows NT-basierten Maschine so auszuführen, als säße er vor der Maschine selbst. Er holt sich quasi den Client-Bildschirm auf seinen Administratorbildschirm. Remote Control läßt sich in einem LAN, in einem WAN sowie über das Internet ausführen; dabei wird eine Vielzahl von Protokollen, u.a. X.25 und ISDN, unterstützt. Um Administratoren in verstärktem Maße bei der Verwaltung von Windows 95-basierten Rechnern zu helfen, wurde der SMS 1.2 mit der Unterstützung von "Shared Applications" für Windows 95 ausgestattet.

Die Funktionen des SMS sind auf eine Server- und eine Client-Installation verteilt. Letztere kann problemlos über das Netzwerk erfolgen. Der Client dient dem Benutzer im wesentlichen zur Einstellung seiner HelpDesk-Optionen, aber auch der Aktivierung von Aufträgen des Paketinstallations-Manager; darüber hinaus erleichtert er die Kommunikation zwischen Client und Server.

Zum Start der Remote Funktionen benötigt der Client USERTSR oder USERIPX. USERTSR wird in Verbindung mit einem Transportprotokoll verwendet, das NetBIOS (NetBEUI oder TCP/IP) unterstützt, und USERIPX mit dem IPX-Transportprotokoll. Darüber hinaus werden, wie vom gesamten BackOffice-Paket, FTP, SMTP, SNMP, SPX, AFP und ODS über die Standard-Ports unterstützt.

SMS 1.2 gibt NT-Systemereignisse an einen SNMP Trap Konverter weiter. Dadurch wird einer beliebigen SNMP Management-Konsole ermöglicht, kritische Systemereignisse auf einem Windows NT-basierten System, wie z. B. zu wenig Speicherplatz oder Sicherheitsverletzungen, zu behandeln und SNMP Traps zu generieren. Ein SNMP Trap kann zu einer Management-Konsole weitergeleitet werden, um den Administrator über das kritische Ereignis zu informieren. Typische Management-Konsolen, die hierzu verwendet werden können, sind etwa HP OpenView, IBM Netview AIX, Digital POLYCENTER, Siemens Nixdorf TransView und SMS.

Die wichtigsten Funktionen sind:

- Aufbau und Unterhalt eines Bestands von Rechner-Hardware und –Software
- Verteilung, Installation und Konfiguration von Software-Paketen
- Verwalten von auf Servern basierenden Anwendungen für das Netzwerk
- Erstellen von Netzwerkprotokollen und Analysen zum Verkehrsaufkommen
- HelpDesk-Unterstützung, Diagnose- und Fernsteuerungs-Funktionen
- Netzwerkmanagement / Unterstützung von Standard-Schnittstellen
- Unterstützung von ODBC, OLE, SNA, MAPI, TAPI, ISAPI

Einige der von SMS unterstützten Standards beinhalten folgendes:

- Desktop Management Interface (DMI), Standard der Desktop Management Task Force
- Management Information File (MIF), ein von DMTF definierter Standard
- Simple Network Management Protocol (SNMP) (Windows NT SNMP-Service)
- NetView von IBM unter Verwendung von SNA Server NetView Alert-Service

SMS beinhaltet folgende Dienste:

- SMS Executive
- SMS Site Configuration Manager
- Inventory Agent
- SMS Site Hierarchy Manager
- Package Command Manager
- SNA Receiver

SMS Executive ist aus Komponenten aufgebaut, die separat oder als Gruppe gesteuert werden können. Die folgenden Komponenten bilden das Programm SMS Executive:

- Inventory Data Loader
- Inventory Processor
- SMS Alerter
- Despooler
- Applications Manager
- Site Reporter
- Maintenance Manager
- LAN-Sender
- RAS-Sender
- SNA-Sender
- Scheduler

2.2.2 Sicherheitsaspekte

Ferninstallationen

Die Rolle des SMS-Verwalters, der üblicherweise auch Administrator des SQL-Servers ist, steht einzigartig da. Es entsteht oft irrtümlich der Eindruck, daß er wenig mehr als ein überschätzter Software-Installierer ist. In einem großen Netzwerk könnte das nicht weiter von den Tatsachen entfernt sein; der Schritt zum allmächtigen Operator ist jedoch nur wenige Konfigurationseinstellungen entfernt. Besonders zu erwähnen sind diesbezüglich die unkontrollierte Generierung von Installationspaketen, wobei die zu installierende Software modifiziert sein kann.

Pakete werden normalerweise aus dem Quellmedium heraus generiert und für die Verteilung vorbereitet. Durch Veränderung dieser Installationsversionen im Ordner SMS_PKGC noch vor der Auftragsfreigabe kann ein Operator z.B. Skripts implementieren, die bei Ausführung der Software ihrerseits Funktionen auf dem Client aktivieren, die normalerweise durch den

Benutzer gesperrt sind. Es folgt, daß zum einen o.g. Ordner durch einen ‚Super-User' auch für die Administratoren gesperrt sein muß, zum anderen die Erstellung von Installationspaketen nur von unveränderten Originalversionen erfolgen darf.

Noch vorsichtiger muß man bei der Verwendung der Remote-Dienste des SMS sein. Hierbei sollten die Empfehlungen des Hamburgischen Datenschutzbeauftragten zu Datensicherungsmaßnahmen bei Fernwartung sowie Fersteuerungs- und Netzwerkkontrollprogrammen (vgl. 11. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten von 1992, Abschnitt 3.3/ 3.4, S.24ff.) berücksichtigt werden.

Dies betrifft vor allem die Vergabe von Rechten für die unbemerkte Installation von Software oder Dateien, z.B. über den (R)SERVICE-Dienst oder mit Hilfe des Package-Control-Managers (PCM) unter Verwendung der mitgelieferten Dateien PCMSVC32.EXE und PCMWIN32.EXE. Diese ermöglichen sogar bei abgemeldetem Client einen Remote-Zugriff, so daß einem Benutzer nicht einmal die Tatsache einer erfolgten Veränderung mitgeteilt wird. Über diese Dienste können beispielsweise auch Dateien in gesicherten Ordnern installiert oder gesicherte Registrierungsschlüssel geändert werden. Ein Benutzerkonto mit Administratorrechten auf dem jeweiligen Rechner, die Berechtigung für Domänen-Benutzer zum Lesen einer PCM-Anweisungsdatei auf dem SMS-Anmeldeserver sowie zum Ausführen eines Installationsprogramms im Paketordner auf dem SMS-Distributions-Server (sofern für die Softwareverteilung ein eigener Server eingerichtet wurde) ist für diese Dienste erforderlich.

Die Gruppe Domänen-Admins sowie Domänen-Benutzer, die auch lokale Administratorrechte haben, erfüllen diese Kriterien und sollten entsprechend eingeschränkt werden. Ein normaler Benutzer, der in der Lage wäre, die Datei PCMSVC32.EXE durch seine eigenen Dienstanweisungen zu ersetzen, könnte sich hierdurch die vollständigen Berechtigungen des Domänen-Admin verschaffen. Benutzer sollten also keinen Administratorzugriff auf ihren Rechner haben, oder, noch besser, der PCM-Dienst ist vollständig von den Clients zu entfernen, bzw. gar nicht erst zu installieren.

Aus Sicherheitsgründen sollte das SMS-Dienstkonto von Zeit zu Zeit an allen Standorten ersetzt werden. Dies geschieht am komfortabelsten mit dem NEWSVCAC-Dienst (New Service Account Creator) gemäß Manual.

Fernsteuerung

Bei den standardisierten Remote-Operationen kann dem Datenschutz hingegen in vollem Maße Rechnung getragen werden. Mit den HelpDesk-Optionen kann der User einzelne Remote-Zugriffsarten (de-) aktivieren. Die Deaktivierung der Optionen hat den Nachteil, daß Zugriffsversuche des Servers zwar abgewiesen, jedoch nicht einmal bemerkt werden.
Bei aktivierten Funktionen wird der Zugriffswunsch des anfragenden Rechners incl. des Netzwerknamens des dort angemeldeten Benutzers übermittelt und eine Erlaubnis des lokalen Users eingeholt:

Abb.8: SMS Sicherheitsabfrage

Darüber hinaus hat der Benutzer ständige Kontrolle über die Aktivitäten des Administrators und kann die Remote-Operation jederzeit abbrechen, sofern er in den notwendigen Rechten (Task/Prozeß beenden) nicht beschnitten wurde.

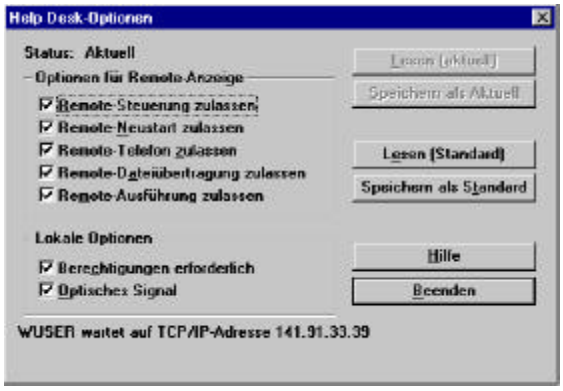


Abb.9: SMS-Client HelpDesk-Optionen

Administration

Der SMS Security Manager ermöglicht es, unterschiedliche Zugriffsrechte für verschiedene Benutzer einzustellen. Nachdem diese Rechte eingestellt sind, können die Benutzer mit dem

Programm SMS Administrator die Arbeiten ausführen, für die ihnen Befugnisse eingeräumt wurden. Auf diese Weise wird es möglich, die unterschiedlichen Aufgaben, die bei der Verwaltung eines SMS-Systems anfallen, auf verschiedene Individuen zu verteilen und mit den Sicherheitsmechanismen des SMS eine unbefugte Verwendung des SMS Administrators zu verhindern. Standardmäßig haben Benutzer keinerlei Zugriffsrechte auf das Programm SMS Administrator.

Die Sicherheitsfunktionen des SMS basieren auf den entsprechenden Mechanismen des SQL Server. Indem man steuert, wer Zugriff auf die SMS-Datenbank und die Tabellen innerhalb dieser Datenbank hat, kann effektiv Einfluß darauf genommen werden, wer die verschiedenen administrativen Funktionen des SMS anwenden darf. Der Microsoft SQL Server bietet verschiedene Datenschutzmodelle an: standard, integriert und kombiniert. Das Modell, das für den SQL Server ausgewählt wird, beeinflußt die SQL Server-Login-ID, unter der man den SQL Administrator startet (vgl. 2.1).

Damit ein Benutzer den SMS Administrator für administrative Aufgaben einsetzen kann, muß für diesen Benutzer eine SQL Server-Login-ID eingerichtet werden und der Benutzer muß ein Zugriffsrecht auf die Standort-Datenbank erhalten. Eine übermäßige Machtstellung kann zunächst einmal unterbunden werden, indem man eine deutliche Trennung der SMS-Datenbanken von anderen, möglicherweise auf dem SQL-Server installierten Datenbanken vornimmt. Im Optimalfall lassen sich die SMS-Daten auf einem eigens für sie bestimmten SQL-Server einrichten.

Eine andere einfache Lösung für Benutzer, die den SQL Server ausschließlich zum Zugriff auf die SMS-Datenbanken verwenden, besteht darin, ihnen mit Hilfe des SQL Enterprise Administrator eine Login-ID einzurichten und die Standort-Datenbank als Standarddatenbank des entsprechenden Benutzers einzustellen. Nachdem eine Login-ID und ein Benutzername für den Benutzer vergeben sind, kann man der betreffenden Person mit Hilfe des SMS Security Manager die gewünschten Rechte einräumen.

Es wird zwischen »No Access« (kein Zugriff), »View Access« (Lesezugriff) und »Full Access« (vollständiger Zugriff) unterschieden:

- No Access (kein Zugriff). Dieses Zugriffsrecht verwehrt dem Benutzer jegliche Möglichkeit, das fragliche Objekt zu betrachten oder zu modifizieren. Wenn einem Benutzer für den HelpDesk beispielsweise No Access zugewiesen wurde, ist er oder sie außerstande, die HelpDesk-Funktionen zu aktivieren. »No Access«, auf Aufträge bezogen, hindert den Benutzer daran, das Fenster »Jobs« zu öffnen. Wenn man »No Access« auf Pakete bezieht, kann der Benutzer das Fenster »Pakete« nicht öffnen, nicht einmal auf Pakete in den Fenstern »Job Properties« oder bei der Definition von Programmgruppen zugreifen.
- View Access (Lesezugriff). Der Benutzer kann das Objekt betrachten, aber keine Objekte dieses Typs anlegen oder vorhandene Objekte modifizieren. Lesezugriff auf Pakete erlaubt es dem Benutzer, Pakete einzusehen und bei der Definition von Aufträgen zu benutzen (falls er vollständigen Zugriff auf Aufträge hat), aber der Benutzer kann die Charakteristiken des Pakets auf keine Weise ändern.
- Full Access (vollständiger Zugriff). Der Benutzer kann Objekte dieses Typs betrachten, anlegen und modifizieren.

Die verschiedenen Objekte in der SMS-Datenbank hängen eng miteinander zusammen. Es ist daher logisch, daß Einstellungen für diese Objekte auch die für andere Objekte erforderlichen Zugriffsrechte beeinflussen, damit Ihre Einstellung ordnungsgemäß funktioniert.

Um die Vergabe von Rechten für SMS-Verwalter zu vereinfachen, sind einige vordefinierte Rollen als Schablonen entwickelt worden. Passende Zugriffsrechte für verschiedene Objekte sind darin unter Berücksichtigung der Objektbeziehungen voreingestellt. Es ist sinnvoll, auf diese Schablonen zurückzugreifen, wenn Zugriffsrechte für die Benutzer vergeben werden sollen.

Schablonen sind für die folgenden Typen administrativer Rollen für den SMS eingerichtet worden:

- Asset Manager
- HelpDesk
- Job Manager
- Network Monitor
- Software Manager
- Tech Support

Handlungsempfehlungen:

- Die bei der Installation eingerichteten Verzeichnisse und Dateien sind auf die Notwendigkeit der vergebenen Berechtigungen hin zu überprüfen und gegebenenfalls zu korrigieren.
- Benutzer dürfen keine Administratorrechte auf ihrem Client haben.
- Die HelpDesk-Optionen sollten auf dem Client durchweg aktiviert sein.
- Keinesfalls darf der PCM-Dienst auf Clients installiert werden, er sollte dort lediglich als Anwendung mit den jeweiligen Benutzerrechten verfügbar sein.
- Das Prinzip der minimalen Zugriffsrechte muß Anwendung finden, d.h. Operatoren dürfen nur genau die Rechte erhalten, die sie zum Ausüben Ihrer Tätigkeit benötigen.
- Die vordefinierten Rechteschablonen sollten als Grundlage für die Rechtevergabe beim SMS-Server dienen.
- Es bietet sich eine Trennung von DBA und SMS-Administrator an.

2.3 Exchange Server

2.3.1 Funktionsbeschreibung

Der Exchange Server wird oftmals als die E-Mail-Komponente des BackOffice-Paketes angesehen. Er bietet jedoch mehr als nur E-Mail. Es handelt sich um ein Produkt zur Lieferung von Meldungen und Informationen zu allgemeinen Zwecken, das den Austausch von Informationen zwischen Personengruppen und die Entwicklung von Arbeitsgruppenanwendungen erleichtert.

Man kann den Exchange Server anfänglich für E-Mail verwenden. Um seine Möglichkeiten jedoch in vollem Umfang auszunutzen, müssen seine Fähigkeiten zur gemeinsamen Nutzung von Informationen und seine ‚Programmable Forms' zum Vorteil genutzt werden.

Der Microsoft Exchange Server 5.5 ist vor allem ein Messaging- und Groupware-Server; Kennzeichen des Servers ist die Integration in Internet-Dienste wie Mail und News, die Unterstützung von E-Mail Funktionen, Gruppenterminplanungen, Groupware Anwendungen, elektronischen Formularen und die integrale Zusammenarbeit mit Windows NT Server, wodurch die Administration leicht zu bewerkstelligen ist.

Neben der EMail-Funktionalität sind auch Directory Service, private und gemeinsam nutzbare öffentliche Ordner, der Microsoft Mail Konnektor und die Migrations-Tools enthalten. Je nach Hardwareausbau können somit kleine Arbeitsgruppen oder Hunderte von Benutzern miteinander kommunizieren und auf gemeinsame Informationen zugreifen. Exchange Server 5.5 erleichtert damit die Kommunikation und den Meinungs- und Informationsaustausch für Organisationen jeder Größe.

Zusätzlich zum SMTP- und MIME- sowie MAPI- und X.400-Support der Version 4.0 werden auch die Internet-Standards POP3 für den Zugriff einfacher Internet-Mail-Clients, HTTP und HTML für den Browser-Zugriff auf Exchange Server, NNTP, LDAP und SSL unterstützt. Exchange Server kann auch als Internet-News-Server fungieren. Dazu ist NNTP als Protokoll für den Nachrichtenaustausch mit Internet-Newsgroups enthalten.

Microsoft Outlook, ein intuitiv zu bedienender Desktop Information Manager, ist als Client für den Exchange Server im Lieferumfang enthalten. Dieses Front-End bietet dem Anwender Funktionalitäten für die Kommunikation und Zusammenarbeit mit anderen Exchange-Nutzern. Dazu gehören die Führung von Journalen zum Dokumentenmanagement, Preview-

Funktionen, die integrierte Gruppenterminplanung, Rückruf oder Ersetzen von Nachrichten sowie die Zusammenarbeit mit Microsoft Office 97. In der Standardversion sind jetzt nicht nur SMTP (Internet Mail Service), NNTP (Internet News Service) sowie MS Mail Konnektor und cc: Mail-Konnektor enthalten, sondern auch ein Notes Konnektor, der Exchange Konnektor und MS Visual InterDev zur Entwicklung von Internet- und Intranet-Lösungen. Outlook als Client zur Exchange-Anbindung ist auch für den 16-Bit- und den Mac-Client integriert. Darüber hinaus sind Active Server Komponenten für Outlook Web Access enthalten.

Der Exchange Server bietet mit dem Lotus cc:Mail Konnektor eine Verbindung zwischen beiden Systemen einschließlich Directory-Synchronisation. Er kann dadurch auch als Gateway-Server für cc:Mail genutzt werden. Im Intranet oder aus dem Internet kann der Zugriff auf den Exchange Server auch über einen Internet-Browser erfolgen. Der SQL-Server unterstützt die Integration in E-Mail durch das SQL-Mail-Leistungsmerkmal. Der Microsoft Exchange Server ist eine Sammlung von Softwareanwendungen, von denen einige Client-basiert und einige Server-basiert sind und die zusammenarbeiten, um Personengruppen und ganzen Organisationen Einrichtungen zur gemeinsamen Nutzung von Informationen zur Verfügung zu stellen. Auf dem Server umfaßt dies sowohl Standard- als auch Wahlkomponenten. Diese Komponenten arbeiten als eine zusammenhängende Einheit. Die meisten Benutzer werden sich nicht bewußt sein, daß die Server-basierten Dienstleistungen, die für die Funktionalität des Exchange Server sorgen, keine einzelnen Programme sind. Dieses Diagramm stellt die Wechselwirkung zwischen den Komponenten in vereinfachter Form dar.

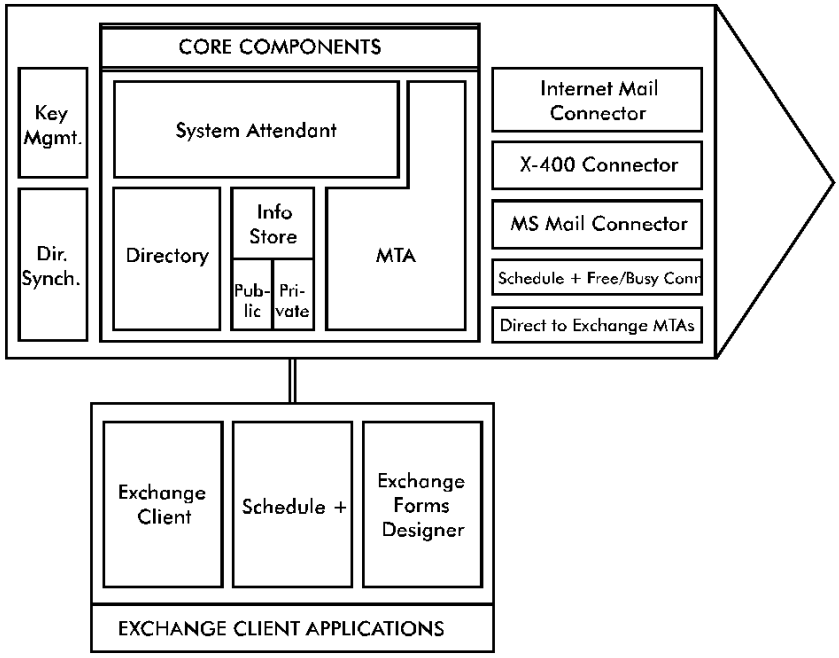


Abb.10: Beziehungen zwischen den Komponenten des Exchange-Servers

Nach Freigabe durch den Administrator können folgende Dienste zur Verfügung gestellt werden:

- Sicherer Zugriff auf E-Mail-Postfächer
- Gesicherter Zugriff auf Kalenderdaten sowohl von Einzelpersonen wie auch von Gruppen
- Zugriff auf Teamwork-Dienste von Exchange. Dazu gehören Diskussionsforen, öffentliche Ordner und Newsgroups. Dieser Zugriff kann nach Einrichtung durch den Administrator auch ohne Authentisierung erfolgen.
- Sicherer Zugriff auf Daten, die im Exchange Directory Service abgelegt sind. Dieser Zugriff dient hauptsächlich zur Remote-Administration.

Eine Anzahl von Client-Komponenten arbeitet auch zusammen, um umfassende Meldungsdienstleistungen für die Benutzer von Desktop-Computern bereitzustellen. Die Client-Komponenten umfassen:

- Exchange Client: Die primäre Komponente, die sowohl Benutzern dabei hilft, ihre Mailboxen zu verwalten, E-Mail zu verfassen und zu senden, als auch benutzerdefinierte Formulare verwendet, um spezielle Arten von Informationen auszutauschen.
- Schedule+: Eine Komponente, die Benutzer- und Gruppenterminpläne anzeigt, die bei der Planung von Ressourcen, wie Konferenzräume oder besondere Ausrüstungsgegenstände, und bei der Projekt- und Aufgabenverwaltung hilft.
- Exchange Forms Designer: Erlaubt Organisationen, benutzerdefinierte Formulare herzustellen, die den Empfang, die Leitung und die gemeinsame Nutzung von speziellen Arten von Informationen erleichtert.

Von Bedeutung ist hier die Zusammenarbeit zwischen den Komponenten, um Informationen zu verwalten und zu liefern. In dieser Hinsicht ist der Exchange Server anderen BackOffice-Anwendungen, insbesondere dem SMS, ähnlich, der auch eine Sammlung von Komponenten verwendet, um Pakete an Desktop-Computer zu liefern.

Die wichtigsten Funktionen auf einen Blick :

- Unterstützung der wichtigsten Internet-Protokolle:
  - SMTP und POP3 für die Übertragung von E-Mails
  - HTTP und HTML zur Unterstützung von World Wide Web
  - LDAP
  - SSL
- Auch aus dem Internet oder im Intranet kann der Zugriff auf den Exchange-Server erfolgen
- Exchange kann als kompletter Internet-News-Server fungieren: NNTP
- Exchange Server unterstützt Apple Macintosh
- Clustering wird unterstützt - hierzu wird die Windows NT 4.0 Server-Version benötigt.
- Wiederherstellung gelöschter Elemente: Löschfristen sind durch den Administrator bestimmbar.
- Interoperabilität:
  + Internet-Mail-Konnektor, der Microsoft-Mail-Konnektor (PC), der Microsoft-Mail-Konnektor (AppleTalk), der Schedule+ Frei/Besetzt-Konnektor und der X.400-Konnektor
  + Lotus Notes Konnektor, unterstützt RTF-Format, bildet Dokumentenverweise (DocLinks) auf URLs ab, mit Notes Directory Synchronisation.
  + PROFS/SNADS (Host) Konnektoren zur Integration mit und Migration von zentralen Mainframe Messaging-Systemen, Directory Synchronisation als Nachtrag.
- Event & Scripting-Service ohne Programmierung
- Geschäfts- und Workflow-Anwendungen erstellen (VB Script, Java u.a.)

2.3.2 Sicherheitsaspekte

Authentisierung und Zugriffsschutz

Die Windows NT-Domänen bieten den Sicherheitskontext, von dem alle Exchange Server-Objekte abhängen. Die Windows NT-Sicherheit ist die Grundlage für alle zugeteilten Genehmigungen und für die Prüf- und Überwachungsmöglichkeiten, die vom Exchange Server geboten werden. Die NT-Serversicherheit identifiziert den Benutzer bei der Anmeldung, die NT-Zugriffskontrolle überprüft Berechtigungen, Protokolle überwachen System- und Benutzeraktivitäten. Die erweiterte Exchange-Server-Sicherheit ermöglicht es dem Benutzer, die Integrität und Authentizität seiner Daten durch Verschlüs-selungsalgorithmen zu sichern.

Es ist im übrigen nicht notwendig, eine 1:1-Abbildung zwischen Standorten und Domänen herzustellen. Man könnte zum Beispiel eine einzige Windows NT-Domäne für die gesamte Organisation benutzen und sich dann immer noch entschließen, mehrfache logische Standorte (vielleicht einen pro Abteilung) für das Exchange Server-System zu benutzen. Umgekehrt könnte ein einziger Exchange Server-Standort mehrere Windows NT-Domänen umfassen. Man denke daran, daß Domänen dazu bestimmt sind, Sicherheit für die gemeinsam benutzten Ressourcen im Netzwerk zu bieten. Exchange Server-Standorte sind dazu bestimmt, die Übermittlung und gemeinsame Nutzung von Informationen zu erleichtern. Die beiden Strukturen können zusammentreffen oder auch nicht.

Um auf einen Exchange Server zugreifen zu können, muß sich der Benutzer nur einmal anmelden. Alle Microsoft Exchange Server-Postfächer sind einem oder mehreren Windows NT-Benutzerkonten zugewiesen. Wenn ein Benutzer sich an einem Microsoft Exchange Server-Computer anmelden möchte, muß die Domäne, in der sich der Server befindet, eine mindestens einseitige Vertrauensstellung mit der Domäne haben, in der sich das Benutzerkonto befindet.

Man kann den Exchange Server jedoch auch so konfigurieren, daß für einige Internet-Protokolle, wie z. B. NNTP (Network News Transfer Protocol), IMAP4rev1 (Internet Message Access Protocol, Version 4rev1) und LDAP (Lightweight Directory Access Protocol) nichtauthentifizierter Zugriff unterstützt wird, damit auch Benutzer anonym auf Informationen zugreifen können, die in Microsoft Exchange Server gespeichert sind. Benutzer, die eine nichtauthentifizierte Verbindung zum Exchange Server herstellen, benötigen für den Zugriff auf Informationen kein Windows NT-Benutzerkonto. Wenn man z. B. bestimmte öffentliche Ordner für IMAP4-Benutzer außerhalb der Organisation freigeben möchten, kann man nichtauthentifizierte Verbindungen aktivieren.

Die Seite »Allgemein« der MTA »Eigenschaften« gestattet, einen Namen und ein Paßwort auf Systemebene für den MTA auf einem Server einzugeben. Dies ist nicht notwendig, wenn man mit anderen Exchange Servern, die schon sichere RPC-Kommunikationsverbindungen verwenden, am gleichen Standort kommuniziert. Dies könnte allerdings erforderlich sein, wenn man mit auswärtigen X.400-Systemen kommuniziert oder, um zusätzliche Sicherheit zu bieten, wenn man mit Exchange Servern an anderen Standorten verbunden ist.

Administration

Ein Servermonitor kann den Status von aktiven Diensten auf einem Server ohne gesonderte Authentisierung überprüfen. Um aber einen Dienst neu zu starten oder die Uhren auf einem Server zu synchronisieren, muß der Kontext des Benutzerprofils, unter dem der Servermonitor läuft, ausreichende Zugangsberechtigung haben. Des weiteren ist diese Art der proaktiven Überwachung 24 Stunden am Tag, 7 Tage in der Woche in vielen Bereichen erforderlich. Da es sich dabei nur um Dienste handelt, die mit einem »Account Logging On« unter Aufsicht ablaufen können, muß eine Möglichkeit gegeben sein, sich automatisch auf Windows NT einzuloggen und die Monitordienste zu starten. Andernfalls müssen Schritte unternommen werden, um zu vermeiden, daß ein Shutdown eintritt oder der Computer die Stromzufuhr verliert und rebooted.

Der Administrator's Guide for Exchange Server zeigt im Detail die Schritte auf, die notwendig sind, um automatisch auf Windows NT einzuloggen und diese Überwachungshilfen zu starten.

Die Sicherheitsauswirkungen einer Maschine, die eingestellt ist, um sich automatisch mit ausreichenden Zugangsberechtigungen auf einen »Account Context« einzuloggen, um Dienste auf einem Server zu unterbrechen und zu starten und Uhren neu einzustellen, ist beunruhigend. Eine solche Maschine sollte zumindest mit einem Screen-Saver ausgestattet sein, der eine extrem kurze Auszeit hat, die die Konsole verschließt, und sie sollte sich an einem Platz mit guter physischer Sicherheit und regulärer menschlicher Präsenz befinden. Da diese Monitore dazu verwendet werden, Grafik-Anzeigen sichtbar zu belassen, damit eine Fehlerbedingung von einem sich in der Nähe befindlichen Operator bemerkt werden kann, kann der Einsatz eines Screen-Savers sich als unmöglich erweisen. Eine Methode der Verschließung der Tastatur könnte statt dessen erprobt werden. Ein offensichtlicher Standort für eine solche Maschine wäre das »Support Center« oder der »Operations Room«, wo die Gefahr einer unberechtigten Benutzung geringer ist. Diesbezüglich sollte zunächst überlegt werden, ob eine permanente proaktive Überwachung im jeweiligen Einsatzbereich überhaupt notwendig ist, oder ob die Reaktion auf entstandene Fehler ausreicht.

Die Verwaltung des Exchange-Servers erfolgt über das Programm Exchange Administrator. Damit können alle Exchange-Server des lokalen Standortes konfiguriert und Server an anderen Standorten betrachtet werden. Die Konfiguration der Benutzerberechtigungen ähnelt dabei sehr dem NT-Benutzermanager:

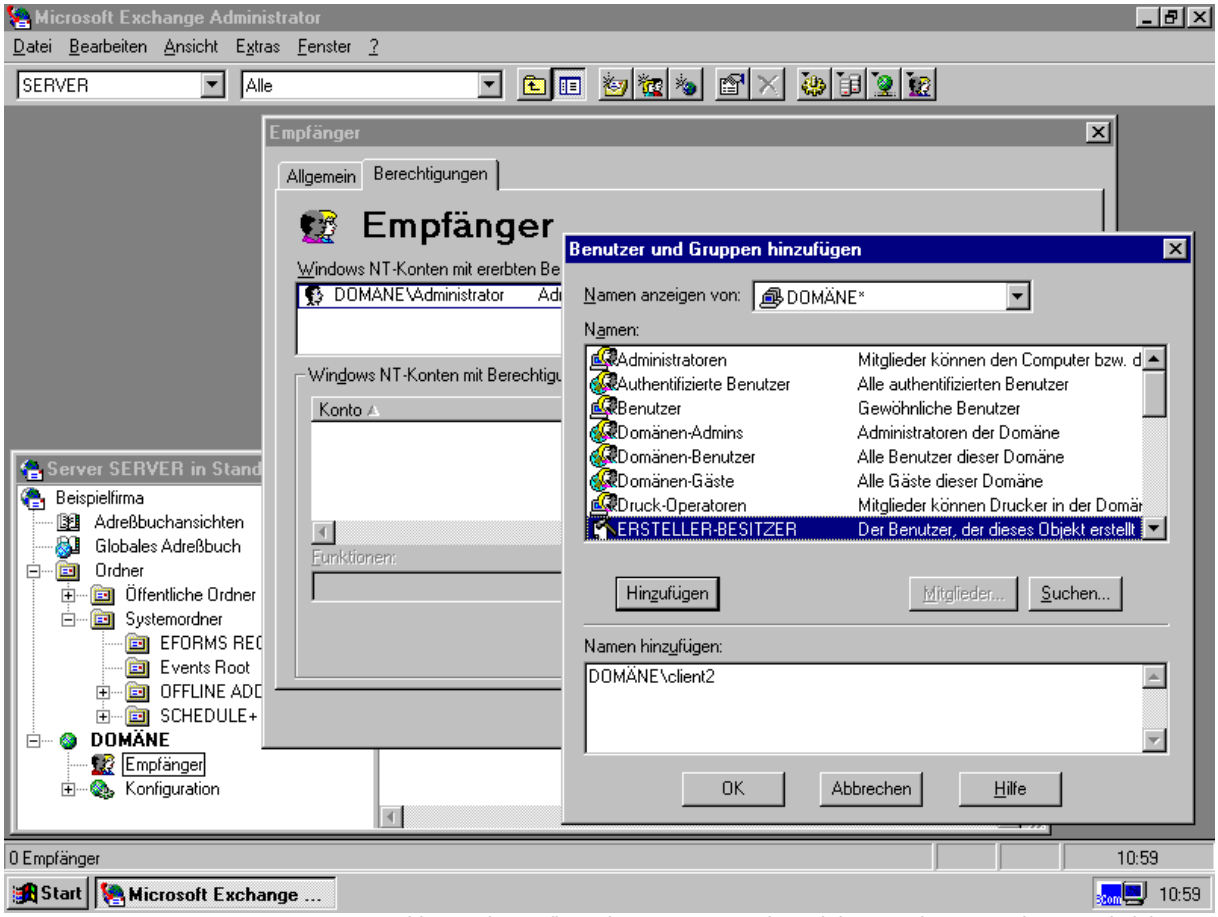


Abb.11: Die Konfiguration von Benutzerberechtigungen im MS Exchange-Administrator

Terminplanung

Schedule+ erlaubt den Benutzern, ihre eigenen Termine auf einem privaten Kalender einzutragen. Sie können Zugriffsberechtigungen einrichten, um anderen Benutzern Zugriff auf ihren Terminplan zu gewähren, wobei der Grad der Zugriffsberechtigung variiert werden kann. Bei der Eintragung von Terminen können diese als privat gekennzeichnet werden, so daß andere Benutzer lediglich erfahren, daß man nicht verfügbar ist, jedoch nicht die Art des Termins. Es ist jedoch nicht möglich, die Funktionalität des Terminkalenders für einen einzelnen Benutzer abzuschalten bzw. ein Kennzeichen für andere Nutzer zu hinterlassen, daß der Scheduler nicht genutzt wird. Es ist möglich, den anzuzeigenden Zeitraum auf null zurückzusetzen oder einen virtuellen Dauertermin anzulegen, dessen zur Einsicht freigegebener Inhalt diejenigen, die einen Termin mittels Schedule+ vereinbaren möchten, darauf hinweist, daß die Funktion vom Besitzer des Kalenders nicht genutzt wird. Alternativ läßt sich die Schedule-Funktion für einen ganzen Exchange-Server deaktivieren.

Verschlüsselung

Microsoft Exchange nutzt im wesentlichen zwei Verschlüsselungstechniken: Eine für jede Kommunikation aufgebaute Verbindungsverschlüsselung sowie eine vom Benutzer veranlasste Ende-zu-Ende-Verschlüsselung nach dem Public-Key Verfahren.

Leztere ermöglicht einen sicheren und verbindlichen E-Mail-Austausch indem die Daten verschlüsselt und die Dokumente digital unterschrieben werden. Dies ist möglich für Exchange-Benutzer verschiedener Organisationen von Client zu Client.

Der Exchange Server verwendet für die Unterstützung der erweiterten Sicherheit öffentliche und private Schlüssel. Schlüssel dienen zum digitalen Unterschreiben und Verschlüsseln von Daten. Jedes Postfach erhält zwei Schlüsselpaare: eins zum Ver- und Entschlüsseln, das andere zum Unterschreiben und Überprüfen. Um im Notfall die Möglichkeit des Key Recovery zu haben, generiert der Key-Management-Server (s.u.) die Verschlüsselungsschlüssel;

Outlook generiert Unterschriftsschlüssel, bei denen die Wiederherstellung von Schlüsseln nur eine unbedeutende Rolle spielt.

Der öffentliche Verschlüsselungsschlüssel dient zum Verschlüsseln einer Nachricht; der öffentliche Unterschriftsschlüssel dient zum Überprüfen der Quelle. Wenn ein Benutzer eine Nachricht verschlüsselt, wird der öffentliche Verschlüsselungsschlüssel jedes Empfängers verwendet. Wenn ein Benutzer eine unterschriebene Nachricht erhält, wird diese mit Hilfe des öffentlichen Unterschriftsschlüssels der Person, die die Nachricht unterschrieben hat, überprüft. Private Schlüssel werden in einer verschlüsselten Sicherheitsdatei (.EPF) auf der lokalen Festplatte des Benutzers gespeichert. Wenn ein Benutzer eine verschlüsselte Nachricht erhält, entschlüsselt der private Verschlüsselungsschlüssel die Nachricht. Wenn ein Benutzer eine Nachricht unterschreibt, wird der private Unterschriftsschlüssel verwendet.

Sicherer als die Speicherung des privaten Schlüssels auf der Festplatte wäre das Verwahren des Schlüssels auf einem mobilen Datenträger, also z.B. einer Magnetkarte oder Diskette. Gerade letztere Lösung ist jedoch nicht überall durchführbar, vor allem da die Diskettenlaufwerke an verschiedenen Arbeitsstationen aus Sicherheitsgründen entfernt oder blockiert werden müssen.

Die für dieses Verfahren erforderliche Schlüsselverwaltung erfolgt auf einem gesonderten Key-Management-Server (KM). Die Schlüsseldateien eines solchen Servers sollten getrennt von anderen Daten gesichert werden. Darüber hinaus sollten für die Aufbewahrung dieser Backups strengere Richtlinien als für normale Sicherungen gelten. Alle Schlüssel in diesen Dateien sind 64-Bit-CAST-verschlüsselt, sind also recht sicher. Man bedenke jedoch, daß diese Dateien sämtliche privaten Schlüssel aller Mitarbeiter der Organisation enthalten.

Als Basis für die Verbindungverschlüsselung dient das CAST 40 Verfahren, ein symmetrisches Verfahren, das außerhalb Nordamerikas nur mit einer Schlüssellänge von 40 Bit ausgeliefert wird. Auch das DES Verschlüsselungsverfahren (56 Bit) gehört nur in Nordamerika zum Lieferumfang des Exchange-Servers.

Abb.12: Einstellung der Verschlüsselungsoptionen

Bei der Beurteilung der Sicherheit dieser Schlüssellängen sollte man insbesondere die Sensibilität der übertragenen Daten berücksichtigen. Für die meisten Anwendungen dürften die mitgelieferten Kryptisierungsverfahren ausreichen, zumal für jede Nachricht ein eigens generierter Schlüssel verwandt wird und auch ein 40 Bit Schlüssel z.Zt. nur mit einigem Aufwand zu knacken ist.

Die Übertragung dieser Schlüssel wird mit dem RSA Verfahren nach X.509 Standard gesichert. Da die Rechenoperationen hierfür jedoch recht aufwendig sind, werden mit dieser Methode lediglich die Schlüssel und nicht die Daten verschlüsselt. Die hierfür notwendigen RSA-Schlüssel werden vom KM-Server generiert und verwaltet.

Schutz von Postfächern

Das unbefugte Einsehen von Postfächern durch (Exchange-) Administratoren ist durch die (Selbst-) Erteilung entsprechender Zugriffsrechte oder durch unwiderrufliche Übernahme des Besitzes an den entsprechenden Objekten möglich. Wurden die Daten zuvor mit dem öffentlichen Schlüssel des Empfängers verschlüsselt, blieben sie natürlich weiterhin unlesbar. Aufgrund des zusätzlichen Verschlüsselungsaufwands dürfte dies jedoch nicht der Normalfall sein.

Die zur Entschlüsselung notwendigen Schlüssel liegen zwar auf dem KM-Server als Sicherheitskopie für Notfälle, können jedoch durch das Vier-Augen-Prinzip geschützt werden.

Für die folgenden Aufgaben läßt sich das Eingeben mehrerer Kennwörter festlegen:

- Hinzufügen oder Löschen von Administratoren, die den KM-Server verwalten dürfen.
- Wiederherstellen oder Widerrufen der privaten Schlüssel eines Benutzers.
- Importieren oder Widerrufen des Zertifikats einer anderen Zertifizierungsstelle.

Handlungsempfehlungen:

- Das Prinzip der minimalen Zugriffsrechte muß Anwendung finden, d.h. Benutzer und Operatoren dürfen nur genau die Rechte erhalten, die sie zum Ausüben Ihrer Tätigkeit benötigen.
- Die bei der Installation eingerichteten Verzeichnisse und Dateien sind auf die Notwendigkeit der vergebenen Berechtigungen hin zu überprüfen und gegebenenfalls zu korrigieren.
- Bei der Kommunikation mit anderen Standorten oder auswärtigen X.400-Systemen ist ein MTA-Passwort einzurichten.
- Bei der Sicherung der Schlüsseldateien des KM-Servers ist mit besonderer Sorgfalt vorzugehen. Die Sicherungen sollten getrennt von der eigentlichen Systemsicherung erfolgen und die Datenträger gesondert, am besten im Tresor, gelagert werden.
- Die Clients sollten so konfiguriert werden, daß sie verschlüsselte RPCs benutzen. Daten, die auf diese Weise über das Netz geschickt werden, können dann wie E-Mails nicht mehr verändert oder eingesehen werden. Für die Verschlüsselung der RPCs wird RC4, ein weiterer 40-Bit RSA Algorithmus, verwandt.
- Für das Hinzufügen oder Löschen von Administratorkonten sowie das Wiederherstellen oder Widerrufen von Schlüsseln sind mehrere Kennworte verschiedener Administratoren einzurichten.
- Die Rechte der Exchange-Operatoren sollten auf ACL-Ebene im Gegensatz zum standardmäßig eingerichteten Administratorkonto so eingeschränkt werden, daß sie sich selbst keine Rechte zum Zugriff auf fremde Postfächer erteilen können.
- Die Administratoren müssen über die Bestimmungen zum Fernmeldegeheimnis gemäß §85 TKG und die resultierenden Rechtsfolgen aufgeklärt und darauf verpflichtet werden.
- Die Benutzer sollten über Funktionsweise und Einsatz der ihnen zu Verfügung stehenden Verschlüsselungsmöglichkeiten sowie über die Möglichkeiten der Einsichtnahme der Administratoren in unverschlüsselt vorliegende E-Mails aufgeklärt werden.
- Zusätzliche Sicherheit kann erlangt werden, indem der Exchange-Server von Anwendungs- bzw. Datenservern in der Domäne getrennt wird. Noch wirksamer ist es, eine eigene Domäne für ihn einzurichten.

2.4 SNA-Server

2.4.1 Funktionsbeschreibung

Die Rolle des SNA Server besteht darin, Konnektivität im Netzwerk zu bieten. Mit diesem Produkt können Desktop-Computer, die auf MS-DOS, Windows, Windows for Workgroups, Windows NT, Macintosh, UNIX oder OS/2 basieren, Verbindung mit IBM AS/400 und IBM Mainframe-Computern aufnehmen. Hierdurch können Unternehmen, ihre Altdaten weiter verwenden, wenn sie auf neuere Computersysteme übergehen. und somit den Mitarbeitern zugänglich machen. Die aktuelle Version läßt dabei bis zu 5.000 Nutzer und 30.000 Sessions gleichzeitig zu.

Der SNA-Server-Verwalter bestimmt die maximale Anzahl an Benutzern und konfiguriert die Umgebung, um ihnen parallele Verbindungen mit dem Host zu ermöglichen. Dazu gehört ggf. auch, Benutzern Privilegien auf dem Mainframe oder den Minicomputern zuzuweisen, für die der SNA Server eine Verbindung bietet. Es können von einem einzigen Bildschirm

aus alle angeschlossenen Server, Verbindungen und Benutzer in einer oder mehreren SNA Server Subdomänen konfiguriert und verwaltet werden. Wesentliche Funktionen sind z.B.:

- Shared-Folders Service: Arbeitsstationen können auch ohne installierte SNA Client Software auf sogenannte "shared folders", die sich auf einer AS/400-Maschine befinden, zugreifen. Dieses Dateisystem ist als Windows NT Server-Dateisystem implementiert; die Dateien auf der AS/400 erscheinen dem Nutzer als normale Windows NT Server-Laufwerke.
- TN3287-Unterstützung: Dieser Dienst erlaubt die Unterstützung der Druckeremulation vieler TN3270-Terminals.
- SNA Server Manager: Diese neue, Windows 95-basierte Benutzeroberfläche erlaubt die zentrale Verwaltung und Bedienung aller Funktionen des Microsoft SNA Server.
- TN5250-Dienst: Eine beliebige TN5250-Emulationssoftware kann sich mit einer AS/400 über SNA Server verbinden, ohne daß auf dieser AS/400 TCP/IP installiert werden muß.
- Host Print-Dienst: Die serverbasierte 3270- und 5250-Druckeremulation erlaubt Großrechner- und AS/400-Anwendungen, auf jedem Netzwerkdrucker unter Windows NT oder NovellNetware auszudrucken. Das spart Kosten für den Systemverwalter und lange Wege ins Rechenzentrum für den Benutzer.
- Die APPC-Syncpoint-Programmierschnittstelle erlaubt die Implementation von stabiler, plattformübergreifender Transaktionsverarbeitung in Bezug auf Host-basierte Datenbanken (z.B. DB2) und Ressource Manager (z.B. CICS).
- Remote Access Service, SNA via RAS, ISDN

2.4.2 Sicherheitsaspekte

Administration

Die Sicherheit des SNA-Server wird vom sog. Dynamic Module (DMOD) gewährleistet. Jegliche Kommunikation mit dem SNA-Server durchläuft dieses Modul, das die Sicherheitskriterien überprüft. Es gibt keine Möglichkeit, sich am DMOD vorbei mit dem SNA-Server in Verbindung zu setzen.

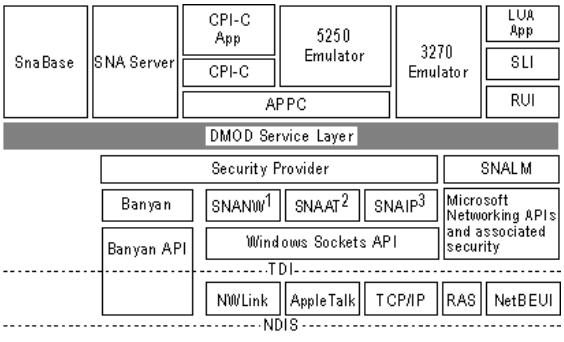
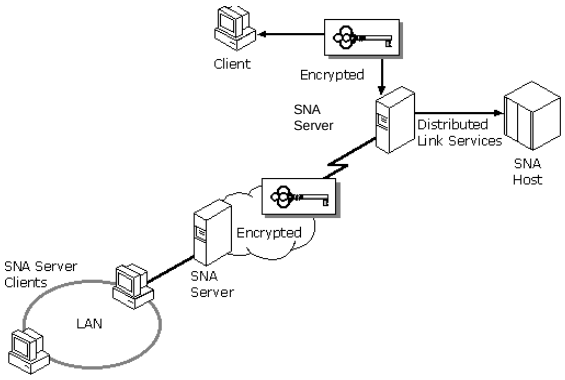


Abb.13: SNA Sicherheits-Architektur

Die SNA-Server-Sicherheit baut jedoch wie alle BackOffice-Komponenten auf der Windows NT Sicherheit auf. Alle gesetzten Protokoll- und Zugriffseinstellungen sind in der Datei \SNAroot\SYSTEM\CONFIG\COM.CFG gespeichert.
Diese Datei und die beiden ausführbaren Programmdateien SNAEXP.EXE und SNACFG.EXE, die für ihre Konfiguration genutzt werden, benötigen besonderen Schutz, der nicht über die normalen NT–Sicherheitseinstellungen konfiguriert werden kann. Hierzu sind die im SNA-Server-Manager vorgegebenen Dialogboxen oder die in der Online-Hilfe beschriebenen systemnahmen Methoden vorgesehen. Bei Manipulation der Berechtigungen über NT-Mechanismen ist die ordnungsgemäße Funktion laut Online-Dokumentation gefährdet.

Verschlüsselung

Um die Sicherheit der Daten zwischen Client und Server zu gewährleisten, kann die Übertragung verschlüsselt werden. Auf diese Weise wird die Sicherheit auf dem Client-Server-Weg für alle Applikationen, die den SNA-Server nutzen, einschließlich 3270/5250 Emulatoren und APPC Logon IDs und Paßwörter, erweitert. Die Verschlüsselung kann für jeden Benutzer gesondert mit Hilfe des SNA Server-Managers eingestellt werden.



Auch Server zu Server Verschlüsselung ist möglich, beispielsweise, um Netzwerk-oder andere WAN-Verbindungen zu sichern. Um Internet- und andere unsichere Verbindungen zu sichern, beherrscht SNA-Server zum einen SHTTP Verschlüsselung, zum anderen SSL, so daß sich auch Telnet- oder FTP-Verbindungen sichern lassen.

Abb.14: SNA-Server Verschlüsselungsmöglichkeiten

Paßwortverwaltung

Paßwörter von IBM Hosts und Windows NT können gemeinsam verwaltet und automatisch synchronisiert werden, um dem Nutzer ein einmaliges, vereinheitlichtes Logon beim Start einer Host-Anwendung oder eines NT-Dienstes zu gestatten. Zwischen SNA Server(n) und Clients wird die Verschlüsselung von Daten und Paßwörtern gemäß dem RC4-Industrie-Standard der Firma RSA mit 128 Bit unterstützt. Da nur Daten zur persönlichen Identifizierung übertragen werden, kann ein solcher Schlüssel verwendet werden, obwohl die derzeit gültigen Exportbeschränkungen der USA ansonsten nur Schlüssel bis 40 Bit Länge zulassen.

Die sog. Host-Security-Integration besteht aus drei installierbaren Komponenten, die auf verschiedene Netzwerkrechner einer Domäne verteilt sein können: Dem Host Account Cache, der Paßwortsynchronisierung (bestehend aus Host- und Windows NT-Konten-Synchronisierungsdienst) und den Security Integration Diensten.

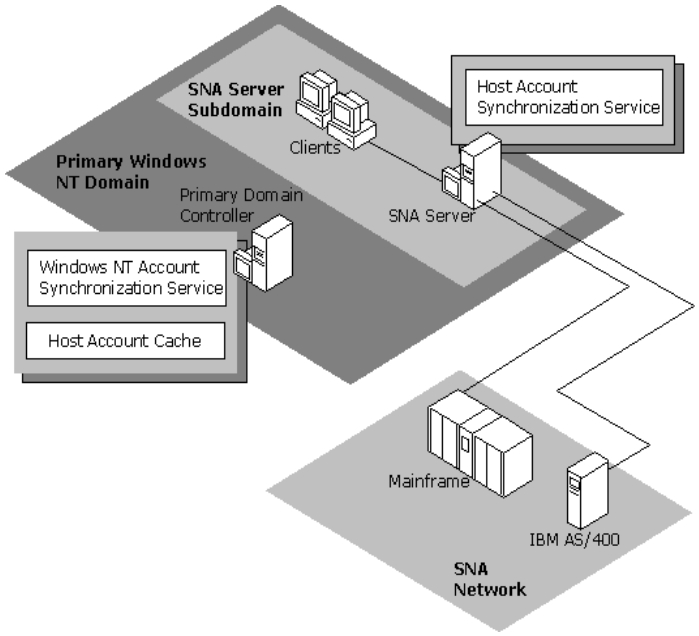


Abb.15: SNA-Server Beispielkonfiguration

Die Synchronisierung geschieht durch den Host Account Cache, der auf dem PDC einer NT-Domäne laufen muß. Er beinhaltet eine verschlüsselte Datenbank, die AS/400 bzw. Mainframe Paßwörter und User IDs in Windows NT Paßwörter und Benutzernamen umsetzt und umgekehrt. Wird das Paßwort an einer Stelle geändert, so erfolgt die Synchronisierung umgehend. Die Host Security Integration wird durch eine ganze Reihe von Funktionen und Aktivitäten umgesetzt. Hierzu gehören das Einrichten einer Host-Sicherheits-Domäne, das Aktivieren von Benutzern, das Zuordnen von Verbindungen zu Sicherheitsdomänen sowie das Aktivieren der Kennwortsysnchronisierung.

Darüber hinaus gibt es ein Bulk Migration Werkzeug, mit dem der Administrator auf Kommandozeilenebene Befehle für mehrere Benutzerkonten gleichzeitig ausführen kann. Mit diesem Werkzeug können auf einfache Weise Benutzerkonten erstellt, gelöscht oder zur Nutzung von SNA-Server freigegeben werden. Korrespondenzen zwischen Host- und NT-Konten können bestimmt, Sicherheitsdomänen angelegt und gelöscht werden.

Handlungsempfehlungen:

• Die Konfigurationsdateien (insb. COM.CFG) müssen sorgfältig geschützt werden.

- Sämtliche Verschlüsselungsmöglichkeiten sind zu aktivieren.
- Vor der Aktivierung des Paßwort-Synchronisierungsservice sollte überlegt werden, inwieweit Sicherheitsaspekte (durch wiederholte Authentifizierung) dem erhöhten Komfort eines einmaligen Logins entgegenstehen. Zu berücksichtigen ist hierbei auch, daß Mitarbeiter, die sich mehrere Paßwörter merken müssen, eher dazu neigen, diese niederzuschreiben oder leicht zu erratene Kennwörter zu verwenden.
- Bei der Arbeit mit dem Bulk Migration-Werkzeug sollte eine sorgfältige Überprüfung der vorgenommenen Einstellungen erfolgen, da diese weitreichende Auswirkungen haben können.

2.5 Proxy-Server

2.5.1 Funktionsbeschreibung

Organisationen, die von einem lokalen Netzwerk aus auf das Internet zugreifen wollen, können einen Proxy Server als Gateway einsetzen. Er hat nicht nur die Aufgabe, allen Anwendern den schnellen Zugriff auf das Internet zu ermöglichen, sondern bietet Administratoren auch die Möglichkeit, die Informationen zu begrenzen, auf die Angestellte im Internet zugreifen können. Oft genutzte Internet-Informationen sind mittels Cache-Funktionen schneller verfügbar und können effektiver aufgerufen werden. Mit dem Proxy Server können verschiedene Caches unter verschiedenen Proxy-Server-Computern verteilt werden. Die Arrays erlauben es, eine Gruppe von Proxy-Servern als einen logisch einzelnen zu behandeln. Mehrere Server können so simultan administriert werden. Der MS Proxy-Server unterstützt verkettete oder gestaffelte Konfigurationen, man kann ihn z.B. hinter einem vorhandenen Firewall einrichten. Die Routing-Funktion ermöglicht außerdem den automatischen Belastungsausgleich sowie Fehlertoleranz, wodurch das Leistungsverhalten verbessert und die Zuverlässigkeit gesteigert wird.

Die Struktur des MS Proxy Server läßt sich mit dem Windows NT Server und dem zum Betrieb notwendigen Internet Information Server durch die kompatiblen Komponenten verbinden und stellt so eine einfache Systemverwaltung sicher. Er ist eng in die Windows NT Serverschnittstelle für Netzwerk-, Sicherheits- und Verwaltungsfunktionen integriert, so daß der Proxy Server von zentraler Stelle mit den gleichen Werkzeugen verwaltet werden kann. Da der Proxy Server alle relevanten Netzwerkprotokolle einschließlich HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), RealPlayer (Streaming Audio/Video), VDOLive (Streaming Video), IRC (Internet Relay Chat) unterstützt, kann weiterhin die vorhandene interne Netzwerktechnologie genutzt werden.

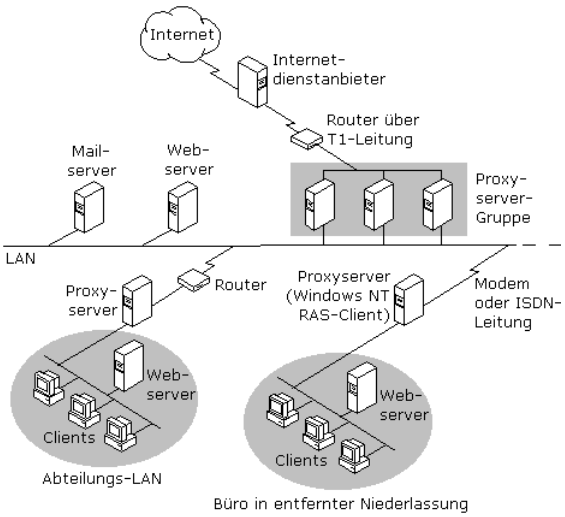


Abb.16: Typische Installation mittelgroßer Organisationen

Der Proxy Server bietet Funktionen, mit denen die Zugänge der einzelnen Arbeitsplätze des LAN zum Internet gesteuert werden können. Es kann festgelegt werden, wer wann auf welche Informationen im Internet zugreifen kann und wer nicht. So kann das Aufrufen bestimmter Adressen von bestimmten Arbeitsplätzen verweigert, der zeitliche Zugriff geregelt oder auch spezielle Internet Dienste freigeschaltet oder gesperrt werden. Gleichzeitig schützt der Proxy Server das LAN gegen Zugriffe von außen. Zudem liefert der Proxy Server Statistiken, welche die Verwendung der Internet Verbindungen dokumentieren. Dies verschafft Transparenz über das aufgerufene Datenaufkommen.

Mit Hilfe von Virtual/Reverse Hosting können einige Webserver hinter dem Proxy Server positioniert werden, was Flexibilität und Sicherheit beim Publishing am Netz erlaubt.

Über die eingebaute dial-on-demand-Funktion kann erreicht werden, daß das Netzwerk nur bei Bedarf mit dem Internet Service Provider verbunden wird.

Einige wesentliche Elemente des MS Proxy Server umfassen :

- Unterstützung der TCP/IP- und IPX/SPX-Protokolle, so daß der Proxy Server im bestehenden Netz eingesetzt werden kann, ohne Veränderungen vornehmen zu müssen.
- Uneingeschränkte CERN-Proxy-Standard-Entsprechung, der die Protokolle HTTP, FTP und Gopher unterstützt, und damit Zugriff auf die größtmögliche Zahl von Browsern und Internet-Anwendungen.
- Unterstützung von SSL (SSL - Secure Sockets Layer), um durch Verschlüsselung und Entschlüsselung einen sicheren Datenaustausch zu gewährleisten.
- WinSock Proxy, womit mit Windows Sockets Version 1.1 kompatible Anwendungen, inklusive LDAP, IRC, SMTP, Microsoft SQL Server, RealAudio und VDOLive, die auf privaten Netzwerken ausgeführt werden, unverändert unterstützt werden.
- Verbesserung der Antwortzeiten und Minimierung des Datenaufkommens im Netzwerk, indem Kopien häufig angeforderter Internet- oder Intranet-Daten auf einem lokalen Rechner zwischengespeichert werden.
- Dynamische Analyse der Zugriffe auf Internet und Intranet, so daß auf Daten, die am häufigsten verwendet werden und zwischengespeichert werden müssen, rasch zugegriffen werden kann.
- Möglichkeit für Administratoren, für alle Objekte im Cache eine Verweildauer (Time-to-Live) festzulegen, damit die Aktualität der Daten und maximale Effizienz sichergestellt werden.
- Verhinderung des unbefugten Zugriffs aus dem Internet auf das private Netzwerk und damit Sicherung sensibler Daten.
- Einschränkung des Zugriffs aus dem privaten Netzwerk auf definierte Internet-Ressourcen über IP-Adresse oder Domain-Name.
- Enge Integration in die Sicherheitsfunktionen und Benutzer-Authentifizierung von Windows NT Server, so daß der Administrator kontrollieren kann, wer im Internet arbeitet und welche Dienste genutzt werden.

2.5.2 Sicherheitsaspekte

Paketfilter-Funktionalitäten

MS Proxy Server agiert als Gateway zwischen einem Intranet und dem Internet. Der Proxy Server ist als zusätzlicher Sicherungsrechner mit Dynamic Packet Filtering einsetzbar, mit zusätzlicher Application Layer Security und Circuit Layer Security. Wird Microsoft Proxy Server im Zusammenspiel mit Routing-Komponenten und Remote Access Service für Windows NT Server benutzt, ist es möglich, sichere Verbindungen mittels Virtual Private LANs (VPNs) zu implementieren. MS Proxy Server unterstützt die Umsetzung individueller Sicherheitskriterien, auch in Zusammenarbeit mit Firewall-Produkten anderer Hersteller. Dabei ist es allein mit dem Proxy-Server möglich, für das interne Netz einen eigenen Class-C Adressraum zu vergeben. Durch die Adressübersetzung ist es denkbar, mit nur einer IP-Adresse nach außen hin zu agieren.

Nicht unterstützt werden Proxy-Routing (ICP), Proxy-ARP, Caching von zugriffsbeschränkten Dokumenten, im Stream-Verfahren übertragenen Daten sowie Precaching. Weiterhin ist eine Blockung von Java, ActiveX oder MIME durch das Produkt allein nicht möglich. Eine Administrationsmöglichkeit über das WWW fehlt.

Benutzerberechtigungen bestimmen, welche Benutzer oder Benutzergruppen Zugang zum Internet über ein bestimmtes Protokoll durch den Web-Proxydienst oder WinSock-Proxydienst erhalten können. Benutzerberechtigungen werden unabhängig von jedem Protokoll gewährt, und die Einstellungen sind jeweils spezifisch für den Web-Proxydienst oder den WinSock-Proxydienst und müssen damit auch gesondert für diese Dienste eingerichtet werden.

Bevor die Benutzerberechtigungen zugewiesen werden, sollten mit Hilfe des Benutzermanagers für Domänen von Windows NT die Benutzergruppen erstellt werden, die die Benutzerkonten enthalten, die Zugang zu einem bestimmten Protokoll oder zu einer Protokollsammlung benötigen. Man kann Gruppen einrichten, um den Internet-Zugang für Benutzer selektiv zu verwalten. Zum Beispiel können Benutzerberechtigungen für Web-Proxyclients die Verwendung der Protokolle FTP, Gopher, HTTP, HTTPS und abgesicherter Protokolle beinhalten. Das Protokoll HTTPS verwendet SSL-Verbindungen (SSL = Secure Sockets Layer).

Protokollierung

Warnereignisse und Protokollfunktionen können nur in engen Grenzen individuell angepaßt werden. Der Proxy Server besitzt drei Dienstprotokolle, in denen Ereignisse aufgezeichnet werden, die vom Web-Proxydienst, WinSock-Proxydienst und Socks-Proxydienst generiert worden sind. Hinzu kommt ein separates Paketprotokoll, in dem Ereignisse aufgezeichnet werden, die sich auf den Paketverkehr im Netzwerk beziehen.

Feldname	Normales Protokoll	Ausführliches Protokoll
Authentifizierungsstatus (ClientAuthenticate)		X
Empfangene Bytes (BytesRecvd)		X
Gesendete Bytes (BytesSent)		X
Client-Agent (ClientAgent)		X
Client-Computername (ClientIP)	X	X
Client-Plattform (ClientPlatform)		X
Client-Benutzername (ClientUserName)	X	X
Zieladresse (DestHostIP)		X
Zielname (DestHost)	X	X
Zielanschluss (DestHostPort)	X	X
Protokolldatum (LogTime)	X	X
Protokollzeit (LogTime)	X	X
Objekt-MIME (MimeType)		X
Objektname (Uri)	X	X
Objektquelle (ObjectSource)	X	X
Vorgang (Operation)		X
Verarbeitungszeit (ProcessingTime)		X
Protokollname (Protocol)	X	X
Proxyname (ServerName)		X
Verweisender Server (ReferredServer)		X
Ergebniscode (ResultCode)	X	X
Dienstname (Service)	X	X
Transport (Transport)		X

Abb.17: Protokollierungsmöglichkeiten des Proxy Server

Alle Protokollinformationen können in einer Textdatei oder in einer ODBC-kompatiblen Datenbanktabelle (wie z.B. Access oder SQL Server) gespeichert werden.

Socks-Unterstützung

Microsoft Proxy Server 2.0 kann als Socks Server oder als Socks Client konfiguriert werden. SOCKS ist ein plattformübergreifender Mechanismus, der die sichere Kommunikation zwischen Client- und Servercomputer gewährleistet. Der Socks-Proxydienst unterstützt SOCKS, Version 4.3a, und ermöglicht den Benutzern den transparenten Zugriff auf das Internet über den Proxyserver. Er dehnt die Umleitungsfunktionen des WinSock-Proxydienstes auf nicht-Windows-Plattformen aus. Er verwendet TCP/IP und kann für Telnet, FTP, Gopher und HTTP verwendet werden. Nicht unterstützt werden das IPX/SPX-Protokoll sowie Anwendungen, die das UDP-Protokoll benötigen. Socks-Proxyclients stellen eine Verbindung mit dem Proxyserver-Computer her, und der Socks-Proxydienst vermittelt Informationen zwischen dem Client und dem Internetserver. Die Sicherheit basiert dabei auf IP-Adressen, Anschlussnummern und Ziel-Hosts. Der Socks-Proxydienst führt keine Echtheitsbestätigung von Clientkennwörtern durch.

Handlungsempfehlungen:

Die im folgenden aufgeführten Optionen allein gewährleisten Sicherheit im Internet nur bedingt. Sie sind lediglich Konfigurationsvorschläge. Insbesondere bei der Verarbeitung sensibler Daten sollte erwogen werden, ob nicht noch eine andere, spezialisiertere Soft-/Hardware herangezogen wird, um die Sicherheit des Internetzugangs zu gewährleisten.

- Das Prinzip der minimalen Zugriffsrechte muß Anwendung finden, d.h. Benutzer dürfen nur genau die Rechte erhalten, die sie zum Ausüben Ihrer Tätigkeit benötigen.
- Es dürfen nur Dienste und Anwendungen ausgeführt werden, die auch benötigt werden. Je weniger Dienste und Anwendungen auf dem System ausgeführt werden, desto weniger

wahrscheinlich ist es, daß ein Fehler in der Administration ausgenutzt werden kann. Unnötige Bindungen von Diensten mit Internet-Adaptern (Netzkarten) müssen gelöst werden.
- Die Zugriffskontrolle muß aktiviert werden. Das Ausführen des Web-Proxydienstes oder WinSock-Proxydienstes ohne Zugriffskontrolle wird als eine nicht sichere Betriebsumgebung betrachtet. Ohne aktivierte Zugriffskontrolle kann keine Echtheitsbestätigung des Kennworts eingerichtet werden.
- DNS- und Gateway-Bezüge in Client-Konfigurationen sollten bereinigt werden. Dadurch werden Clients davon abgehalten, den Proxyserver für den Internet-Zugang zu umgehen. Wenn DHCP verwendet wird, sollten dieselben Verweise entfernt werden, um auch DHCP-Server vom Zugriff auf Adressen außerhalb des internen Netzwerks abzuhalten.
- Externe IP-Adressen dürfen niemals in die lokale Adressentabelle (LAT) geschrieben werden. Wenn man externe IP-Adressen zur LAT hinzufügt, wird das gesamte interne Netzwerk für Internet-Server und Internet-Clients offengelegt. Dadurch kann die Sicherheit des internen Netzwerks massiv gefährdet werden.
- Netzlaufwerk-Zuordnungen zu anderen Remote-Servern sollten im internen Netzwerk nicht verwendet werden. Das ist besonders wichtig, wenn derselbe Computer für den Proxyserver und für Veröffentlichungen im Web mit dem IIS verwendet wird.
- Der Server-Dienst von Windows NT, also das Protokoll SMB (Server Message Block) darf nicht über das Internet ausgeführt werden.
- Die Anschlüsse 1024 bis 1029, die von den TCP/IP-Diensten für die RPC Empfangsbereitschaft (Remote Procedure Call) an der Internet-Schnittstelle verwendet werden, sollten deaktiviert werden. Man kann alle Anschlüsse deaktivieren, die für die RPC Empfangsbereitschaft an der externen Netzwerkschnittstelle verwendet werden. Daraufhin sind diese Anschlüsse nicht mehr für das Internet sichtbar, und RPC-Empfang ist nur über die interne Netzwerkschnittstelle möglich.
- Aus Sicherheitsgründen ist die bevorzugte Konfiguration von Microsoft Proxy Server die als eigenständiger Server in der aktuellen Domäne.
- Wenn Remote Access Service (RAS) von Windows NT nach der Installation des Proxyservers installiert wird, ist das IP-Forwarding aktiviert. Das IP-Forwarding muß nach der Installation von RAS gegebenenfalls deaktiviert werden.

Die folgenden Empfehlungen müssen den individuellen Gegebenheiten angepaßt werden; es sind Vorschläge für mögliche Konfigurationen die nicht direkt umgesetzt werden müssen.

- Die Empfangsbereitschaft auf empfangenen Ports (Dienstanschlüssen) kann deaktiviert werden. Dadurch werden Internet-Benutzer davon abgehalten, Verbindungen über Dienstanschlüsse aufzubauen, die nicht speziell für den ankommenden Zugriff aktiviert sind.
- Man kann den Server-Dienst dazu verwenden, neue Dokumente von Computern im internen Netzwerk hochzuladen, aber andererseits nicht wünschen, daß Benutzer aus dem Internet direkten Zugang zum Server-Dienst erhalten. Wenn man den Server-Dienst im internen Netzwerk verwenden muß, deaktiviert man die Bindung mit dem Server-Dienst auf jeder Netzwerkkarte, die mit dem Internet verbunden ist.
- Die IP-Weiterleitung auf dem Server kann unterbunden werden. Die IP-Weiterleitung (IP-Routing) erlaubt es normalerweise, daß Pakete in das interne Netzwerk weitergeleitet werden. Deaktiviert man dieses Leistungsmerkmal auf dem Server, werden keine Pakete durch den Proxyserver in das interne Netzwerk weitergeleitet.

2.6 Internet Information Server

2.6.1 Funktionsbeschreibung

Microsoft Internet Information Server (IIS) stellt ein zentral verwaltetes System dar, mit dem die Installation, Verwaltung und der Betrieb mehrerer Server mit mehreren IIS-Serviceleistungen von einem einzigen NT-Rechner aus möglich ist. Der Internet Information Server ist eine Plattform, die auf einige Vorteile der NT Technologie zurückgreift, z. B. die

Zugriffsrechtestruktur, Netzwerkeinbindung und eine Unterstützung von ODBC-Datenbanken. Der IIS ist fester Bestandteil des NT Server 4.0 und z.B. zum Betrieb des MS Proxy-Servers zwingend erforderlich. IIS wird als Satz integrierter NT Server-Serviceleistungen ausgeführt, die die eingebauten Eigenschaften von NT Server nutzen (wie den Service Manager, Performance Monitor und die Windows NT Server Sicherheit). Man kann ihn als Web-Server für Inhouse Publishing oder Internet nutzen.

Eine der wichtigsten Eigenschaften des IIS ist neben der Einbindung ins Internet die anwenderfreundliche und übersichtliche Organisation der internen Informationsstruktur. Dies geschieht z. B. durch gespiegelte Web-Server oder das Verwalten von mehreren virtuellen Stammverzeichnissen - auch wenn diese sich auf mehrere Web-Server verteilen.

Internet Dienste wie FTP und Gopher sind im IIS bereits fest integriert. Mit Hilfe des Internet-Datenbank-Konnektors können Datenbankanwendungen über die ODBC Schnittstelle integriert und mit einem Web-Browser als Client aufgebaut werden. Die ODBC-Schnittstelle erlaubt über .idc-Dateien einen unkomplizierten Zugang zu verteilten Datenbanken über normale HTML-Seiten.

Der Internet Information Server verfügt bereits standardmäßig über diverse Funktionen: Die gleichzeitige Unterstützung für NCSA und CERN Style Image Map Files erleichtert den Import von UNIX-Systemen. Der Internet Information Server kann dabei auch Nachsendungen von Image Map Lookups versenden. Die gesamte Verwaltung des IIS kann über die Internet Server-Programmierschnittstelle vollständig über einen einfachen Web-Browser durchgeführt werden. Der Internet Server Manager kann alle Internet Information Server im Netz mit einem einzigen Tool administrieren. Auf einem einzigen ISS können mehrere virtuelle Stammverzeichnisse, die sich auch auf anderen Computern im Netz befinden dürfen, verwaltet werden. Mehrere virtuelle Web Server bilden eine einzige Verwaltungseinheit und einen Betriebssystemprozeß.

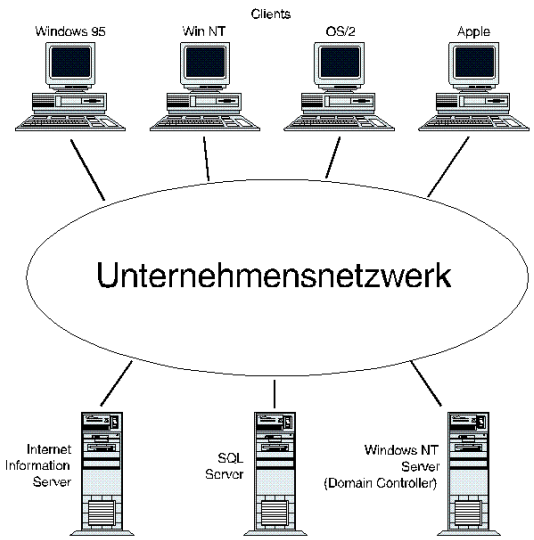


Abb.18: Typische Konfiguration eines Netzwerkes mit IIS

Selbst nach einer Netzwerkunterbrechung kann eine Datei weiterbearbeitet werden. Über den Index Server (siehe 2.7) sind neben einer Inhaltsindizierung auch Suchmöglichkeiten für HTML-Dateien und Office-Dokumente in verschiedenen Sprachen integrierbar.

Der IIS bedient drei Basis-Services, WWW, FTP und Gopher. Man kann den IIS auf verschiedene Arten konfigurieren. Es ist möglich, den Service eines einzigen logischen IIS auf mehr als einem Compu-

ter auszuführen. Ein Client-Computer würde annehmen, daß der Service von einer einzigen Maschine zur Verfügung gestellt wird. Hier sind zwei Möglichkeiten zum Implementieren des IIS-Service:

- Server: Jede Maschine mit allen drei IIS-Basis-Services. Man kann zum Beispiel drei IIS-Abteilungsmaschinen haben, die alle drei IIS-Serviceleistungen ausführen.
- Serviceleistungen: Unterschiedliche Maschinen, die IIS-Service für WWW, FTP und Gopher ausführen. Man kann z. B. drei IIS-Maschinen haben, wobei die eine WWW Service, die andere nur FTP-Service und die dritte nur Gopher-Service ausführt.

Die Wahl hängt von der Verwendung der IIS-Sites ab. Man entscheidet sich möglicherweise für IIS-Abteilungssites zur Bearbeitung der Internet-Bedürfnisse jeder einzelnen Abteilung. In diesem Fall benötigt man IIS-Maschinen, die alle drei Serviceleistungen für jede Abteilung

anbieten. Wenn man sich dafür entscheidet, organisationsweite IIS Sites einzurichten, sollte man eine Maschine für jeden Service haben, um den Netzwerkverkehr zu verwalten und um die Maschinen je nach Typ zu verwalten und zu warten.

Der *WWW-Service* umfaßt folgende Eigenschaften:
- Den NT Server Directory Service, der Benutzerkennungen und Kennwörter für geschützte WWW-Dokumente erfordert.
- Integration mit dem NT-Sicherheitsmodell, das einen vergleichsweise sicheren WWW-Server ermöglicht.
- Virtuelle Verzeichnisse, mit deren Hilfe es möglich ist, bestehende Dateien von Windows NT und NetWare Server für die Anzeige in Web-Browsern zu veröffentlichen.
- Eingebaute SSL-Sicherheitmit 40 Bit Verschlüsselungsstärke).
- Virtuelle Serverfähigkeiten, die mehrere WWW-Sites auf einem NT Server-Computer gestatten und somit die Verwaltung erleichtern.
- Grafische Verwaltung aller Aspekte durch den Internet Service Manager.

Der WWW-Service in IIS unterstützt die Ausführung von Programmen auf dem Server (CGI-Schnittstelle) und das Erstellen und Verwenden dynamischer Web-Pages. Wenn man einen neuen WWW-Server installiert, erstellt IIS automatisch ein Stammverzeichnis für den Server. Dem Stammverzeichnis \INETSRV \WWWROOT wird hierbei standardmäßig der Aliasname »Home« gegeben.

Zusätzlich zur Verwendung des Home-Verzeichnisses zum Veröffentlichen von Informationen kann auch das Konzept der virtuellen Verzeichnisse verwendet werden. Mit virtuellen Verzeichnissen können Informationen über Verzeichnisse hinweg verteilt werden, die keine Unterverzeichnisse des Verzeichnisses »Home« sind. Sie können auch verwendet werden, um Informationen auf einem anderen Laufwerk oder Netzwerklaufwerk abzulegen.

Mit Hilfe des virtuellen Servers kann mehr als einen WWW-Server auf derselben Maschine laufen. Standardmäßig hat jede Maschine eine einzige Domäne und eine IP-Adresse. Der virtuelle Server gestattet, zusätzliche IP-Adressen und Domänennamen an den Server anzuhängen, damit es so aussieht, als würden mehrere Server verwendet. Es könnten also WWW-Server für verschiedene Abteilungen in einer Organisation erstellet werden, ohne je eine eigene Maschine für den Web-Server einzurichten.

Mit dem Gopher-Service in IIS können Informationen von großen archivierten Dateien veröffentlicht werden. Der IIS-Gopher-Service unterstützt die Eigenschaften des Gopher-Standard. Außerdem unterstützt der Gopher-Service in IIS die »Gopher + Selector«-Zeichenketten, mit denen Clients zusätzliche Informationen vom Server erhalten können, wie beispielsweise den Verwalternamen des Gopher-Servers. Man kann auf dem Gopher-Server markierte Dateien verwenden, um Verbindungen zu anderen Gopher-Servern im Unternehmen oder auf dem Internet herzustellen.

Der der im Internet Information Server eingebaute FTP-Server unterstützt Anonymous FTP zum Zugriff auf das Internet, um Dateien herauf- und herunterzuladen zu können.

Der Internet Service Manager ist ein grafisches Programm zur zentralen Verwaltung aller Funktionen des Internet Information Server. Der Internet Service Manager bietet eine gemeinsame Verwaltungsstelle für die Verwaltung des WWW-Server- Service, des FTP Service und des Gopher Service.

Mit dem Internet Database Konnektor bietet IIS Konnektivität mit der Microsoft SQL Server-Datenbank über die »Open Database Connectivity« (ODBC)-Schnittstelle. Der Internet Database Connector gestattet Organisationen die Entwicklung datenbankaktivierter WWW-Anwendungen. Das ist eine wichtige Eigenschaft, mit der Benutzer auf Unternehmensdaten von einem beliebigen Ort der Welt mit Hilfe des Internet zugreifen können. Die IIS-Integration mit SQL Server über ODBC Gateway bietet einen Ansatz für die Entwicklung datenbankaktivierter Internet-Anwendungen.

Wichtige Features im Überblick :

- Vergabe von individuellen Zugriffsrechten
- Zenrales System Management
- Skalierbarkeit und Portierbarkeit der Daten
- Interaktiver Zugriff auf Datenbankanwendungen
- Unterstützung von E-Mail-Funktionen von Exchange
- World Wide Web Service
- Internet Service Manager
- Gopher Service
- Internet Database Connector
- FTP Service

2.6.2.Sicherheitsaspekte

Die integrierte Sicherheit wird über den Server-Verzeichnisdienst von Windows NT auf Benutzer- und Objektebene und über ESSL (Enhanced Secure Sockets Layer) auf Netzwerkebene gewährleistet. Alle Dienste können protokolliert werden, hierzu kann entweder ein Textformat oder aber der SQL Server verwendet werden.

WWW-Server

Standardmäßig meldet der Webserver alle Benutzer mit Hilfe eines sogenannten anonymen Kontos an. Während der Installation erstellt der Server ein besonderes Konto für anonyme Benutzer, das den Namen IUSR_Computername erhält. Es kann verhindert werden, daß Benutzer ohne Authentisierung auf zugriffsbeschränkte Inhalte zugreifen. Der Benutzer wird aufgefordert, eindeutige Informationen zum Benutzernamen und zum Kennwort einzugeben, die einem gültigen NT-Benutzerkonto entsprechen müssen. Dieses Konto unterliegt den Datei- und Verzeichnisberechtigungen des NTFS Dateisystems, durch die die Zugriffsebene für das Konto definiert wird.

Die SSL-Sicherheitsfunktionen des Webservers können verwendet werden, um die Benutzer zu authentifizieren. Bei dieser Form der Authentifizierung wird der Inhalt einer verschlüsselten digitalen Identifikation überprüft, den der Webbrowser des Benutzers während des Anmeldevorgangs übermittelt.

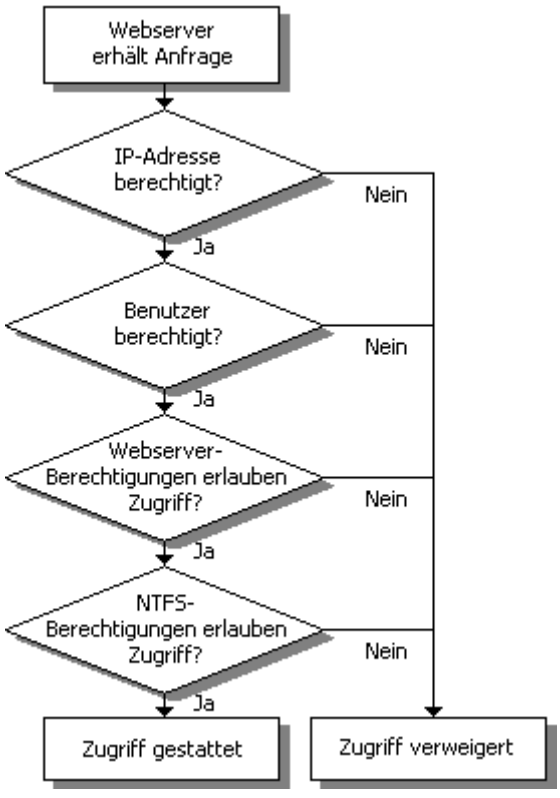


Abb.19: Authentifizierung des Web-Zugriffs

Die Benutzer erhalten diese digitale Identifikation, die als Clientzertifikat bezeichnet wird, in den meisten Fällen von einer Organisation, die von beiden Seiten anerkannt wird (Trusted Third Party-TTP). Die Clientzertifikate enthalten in der Regel Informationen, die den jeweiligen Benutzer und die Organisation identifizieren, die das Zertifikat ausgegeben hat.

Programmschnittstellen

Ein wichtiger Aspekt eines WWW-Servers ist die Fähigkeit, Programme im Rahmen einer Hypertext-Verbindung auszuführen. Zusätzlich zur Verwendung von Hypertext-Verbindungen zum Ausführen von Anwendungen können Benutzer auch Anwendungsausführungen auslösen, indem sie ein HTML-Formular ausfüllen und es zur Verarbeitung dem Server vorlegen. Die Fähigkeit, Programme auf dem WWW-Server auszuführen, erhöht das Risiko, daß Benutzer in das System »einbrechen« können. Man sollte entsprechend vorsichtig sein und Benutzer davon abhalten, daß sie Lese-/Schreibzugriff auf die ausführenden Programm- und Skriptdateien erhalten.

Der WWW-Service im IIS unterstützt das Konzept vollständig, Server-basierte Anwendungen auszuführen, indem er den Standard Common Gateway Interface (CGI) unterstützt.

IIS unterstützt auch ein eigenes Application Programming Interface (API) zum Schreiben Internet-aktivierter Anwendungen, das »Internet Server Application Programming Interface« (ISAPI) genannt wird. Man kann jede beliebige Sprache, wie C/C++ oder Visual Basic, verwenden, um Anwendungen zu schreiben, die die CGI- oder ISAPI-Schnittstelle verwenden.

Absolute Vorsicht muß man walten lassen, wenn man Benutzern gestattet, Dateien auf den Server zu kopieren. Man vergewissere sich, daß man alle Dateien auf Viren überprüft. Ankommende Dateien sollten auf ein einziges Verzeichnis kopiert werden, um den Überprüfungsprozeß der Dateien zu erleichtern.

FTP-Server

Die im IIS integrierte Sicherheit gestattet den Verwaltern, den Zugriff auf den FTP-Service basierend auf Benutzerkennungen und Kennwörtern für Dateien und Verzeichnisse einzuschränken. Zum Herstellen einer FTP-Verbindung zum Webserver müssen sich die Benutzer mit einem Benutzernamen und einem Kennwort anmelden, die zusammen einem gültigen NT-Konto entsprechen. Wenn der IIS die Identität eines Benutzers nicht überprüfen kann, gibt er eine Fehlermeldung zurück. Die FTP-Authentifizierung ist nicht sicher, da die Benutzer das Kennwort und den Benutzernamen in unverschlüsselter Form über das Netzwerk übermitteln. Dadurch kann auch die Sicherheit anderer NT-Dienste gefährdet werden.

Interaktion mit dem SQL-Server

Die Integration der NT Server-Sicherheitseigenschaften in SQL Server und IIS bietet eine sichere Datenbankkonnektivitätsoption. Wenn Benutzer Windows NT Security verwenden, können datenbankaktivierte Anwendungen vom NT Server und SQL Server authentiziert werden, bevor sie Zugriff auf Unternehmensdaten erhalten. Die Optionen der Internet Security, »Secure Sockets Layer« (SSL), »Secure Transaction Technology« (STT) und »Cryptography Application Programming Interface« (CAPI) bieten auch eine Methode zur Durchführung sicherer Transaktionen auf dem Internet. Außerdem ermöglichen sie die Entwicklung Internet-aktivierter Anwendungen, die die derzeit durch den Exchange-Server unterstützten Verschlüsselungs- und Sicherheitstechnologien verwenden.

Besondere Vorsicht ist jedoch geboten, wenn neben dem IIS auch der SQL-Server installiert wurde. Wenn der RDS des IIS installiert wurde, was bei der Installation über das ‚NT Option Pack' standardmäßig der Fall ist, ergeben sich insbesondere bei eingerichteten OLE-DB-Providern erhebliche Sicherheitsdefizite (vgl. 2.1). Der Remote Data Service ist also unbedingt abzuschalten.

Handlungsempfehlungen:

- Das Prinzip der minimalen Zugriffsrechte sollte Anwendung finden, d.h. Benutzer sollten genau die Rechte erhalten, die sie zum Ausüben Ihrer Tätigkeit benötigen.
- Es sollten sichere Authentifizierungsmechanismen verwandt werden, wenn anonymisierter Zugriff nicht ausdrücklicher Zweck des Servers ist.
- Wenn der Webserver von einem Remotecomputer aus verwaltet wird, sollten SSL-Sicherheitsfunktionen verwandt werden.
- Der NT Server mit IIS kann vom Rest des Unternehmensnetzwerks getrennt werden, indem ihm seine eigene Domäne zugewiesen wird. Es wird dann eine einseitige Vertrauensbeziehung eingerichtet. Benutzern des Organisationsnetzwerks wird der Zugriff auf die IIS-Maschinen gestattet, Benutzerkonten von der Domäne, die die IIS-Maschinen enthält (besonders Gästen) wird jedoch untersagt, auf das Netzwerk zuzugreifen. Alle IIS-Serviceleistungen werden hierbei im Sicherheitskontext eines Server-Kontos von der nichtvertrauten Domäne aus ausgeführt, die den IIS Server enthält.
- Es sollte sich vergewissert werden, daß die IIS-Maschine mit den notwendigen Zugriffsbeschränkungen versehen wurde, um nichtautorisiertes Kopieren oder Ändern zu vermeiden.

- Es sollten, soweit möglich, immer verschlüsselte Kennwörter im Internet verwandt werden.
- Der RDS muß unbedingt deaktiviert werden, wenn ein SQL-Server installiert ist.
- Alle durch FTP übertragenen Dateien sollten auf Viren überprüft werden.
- Es sollte ein Firewall eingerichtet werden, um unerlaubten Zugriff auf das Netzwerk zu vermeiden. Firewalls, Screening Router und andere ähnliche Sicherheitsmaßnahmen können den Zugriff auf IIS Sites beschränken. Man kann z.B. Datenverkehr, basierend auf IP-Adressen oder Sicherheits-schlüsseln, einschränken:

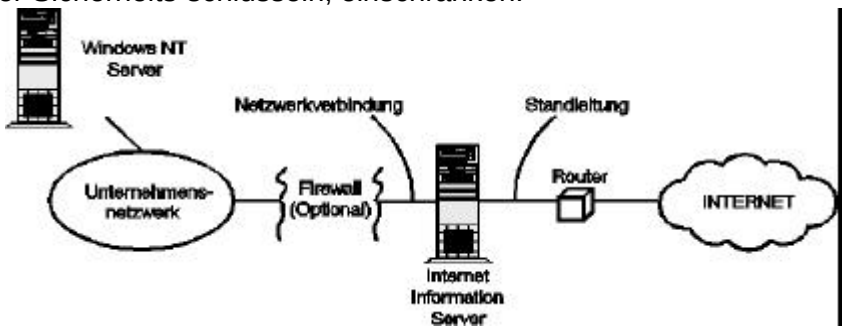


Abb.20: Der IIS hinter einem Firewall

2.7 Index Server

Microsoft Index Server ist eine Lösung, um vom Internet Information Server (IIS) oder von den Microsoft Peer Web Services (PWS) verwaltete Inhalte zu durchsuchen und zu indizieren. Als Zusatzmodul für IIS und PWS wurde der Microsoft Index Server so entworfen, daß er den gesamten Text und die Eigenschaften von Dokumenten indizieren kann, die von einem IIS (oder PWS) Server verwaltet werden. Der Index Server kann Dokumente indizieren, die sich in unternehmensinternen Intranets oder auch auf beliebigen Datenträgern im Internet befinden, auf die über einen UNC-Pfad (UNC=Uniform Naming Convention) zugegriffen werden kann. Clients können Abfragen formulieren, indem sie über einen beliebigen Browser für das World Wide Web die Felder eines einfachen Abfrageformulars ausfüllen. Der Web Server leitet das Abfrageformular an das Abfragemodul weiter, das die zugehörigen Dokumente ermittelt und das Suchergebnis in Form einer Web-Seite an den Client zurückgibt. Im Unterschied zu anderen Systemen zur Inhaltsindizierung kann der Index Server sowohl den Text als auch die Eigenschaften von formatierten Dokumenten indizieren, wie zum Beispiel Dokumente, die mit MS Word oder Excel erstellt wurden. Auf diese Weise kann man bestehende Dokumente im Intranet veröffentlichen, ohne sie in das HTML-Format konvertieren zu müssen.

Bei der ersten Installation des Index Servers wird ein Katalog mit einer Zugriffskontrolliste (ACL) eingerichtet, die nur dem Administrator und den Systemdiensten Zugriff gestattet. Dadurch wird zum einen sichergestellt, daß unbefugte Benutzer die Dateien im Katalog nicht als Teil ihrer Abfrage sehen können, wenn das Katalogverzeichnis sich in einem virtuellen Stammverzeichnis befindet. Der Schutz des Katalogverzeichnisses ist auch wichtig, um unbefugten Benutzern (die Zugriff auf den Server über freigegebene Verzeichnisse erhalten könnten) daran zu hindern, den Inhalt des Katalogs zu sehen.

Wenn ein weiteres Katalogverzeichnis manuell erstellt wird, sollte sichergestellt werden, daß dieses und die in ihm erstellten Dateien entsprechende Zugriffsbeschränkungen erhalten. Ein Katalogverzeichnis sollte ausschließlich den Zugriff für den Administrator und für das Systemkonto gewähren. Da der Index Server als ein Dienst ausgeführt wird, ist der Systemzugriff erforderlich.

Wenn Dokumente indiziert werden, werden alle Zugriffskontrollen für ein Dokument im Katalog geführt und gegen die Client-Rechte geprüft. Wenn ein Client keinen Zugriff auf ein Dokument hat, dann wird das Dokument nicht in dessen Abfrage-Ergebnisse mit einbezogen; es gibt für ihn keinen Hinweis darauf, daß dieses Dokument existiert.

Damit die Zugriffskontrolle korrekt angewendet werden kann, ist es nötig, daß für jeden Client vor der Bearbeitung seiner Abfrage eine Echtheitsbestätigung durchgeführt wird. Der einfachste Weg, die Echtheitsbestätigung eines Clients sicherzustellen, ist das Anbringen einer entsprechenden Zugriffskontrolle auf dem Formular, das eine Abfrage übermittelt. Eine Zugriffskontrolliste könnte auch der in einer Abfrage verwendeten .idq- oder .htx-Datei zugeordnet werden. Je nach Konfiguration des Internet Information Servers (IIS) können ein oder mehrere Mechanismen der Echtheitsbestätigung verwendet werden. Dies sind: Echtheitsbestätigung über NT-Challenge/Response-Verfahren, einfache Echtheitsbestätigung, nichtauthentifizierte Anmeldung.

Bei einem Intranet, das vollständig aus Windows NT-Workstations und Windows NT-Servern besteht, ist das Windows NT- Challenge/Response-Verfahren die bevorzugte Art der Echtheitsbestätigung. Hierbei wird das Kennwort des Clients nicht im Klartext über das Netzwerk übertragen.

Wenn die anonyme Anmeldung erlaubt ist, wird sie als Vorbelegung so lange verwendet, wie die Client-Zugriffe auf Dateien mit den Zugriffsrechten des anonymen Anmeldekontos übereinstimmen. Wenn der Versuch unternommen wird, Zugriff auf ein Dokument zu erhalten, für das der anonyme Benutzer keine Zugriffsrechte hat, wird ein Dialogfeld für die Echtheitsbestätigung angezeigt (sofern ein alternativer Mechanismus für die Echtheitsbestätigung zur Verfügung steht). Daraufhin kann der Client seine Echtheit bestätigen und damit die Zugriffsrechte für die entsprechende Datei erhalten, die ihm andernfalls verwehrt würden. Die Echtheitsbestätigung aller Clients, die auf den Server zugreifen, kann erzwungen werden, wenn das anonyme Anmeldekonto deaktiviert wird.

Wenn beim IIS und den PWS der Index Server für den Zugriff auf ein virtuelles Stammverzeichnis und dessen Indizierung konfiguriert ist, wird der Zugriff auf dieses virtuelle Stammverzeichnis und auf die in ihm enthaltenen Dokumente durch das Konto bestimmt, das für den Zugriff auf das freigegebene Remote-Verzeichnis konfiguriert wurde. Jedes zugängliche Dokument wird indiziert und jedem Client zur Verfügung gestellt, der eine Verbindung zum Server herstellt. Die oben beschriebenen Zugriffsüberprüfungen für Abfrage-Ergebnisse werden in diesem Fall ausdrücklich deaktiviert. Bei der Indizierung virtueller Remote-Stammverzeichnisse sollte man sich bewußt sein, daß die Dokumente in diesem Verzeichnis unbeabsichtigt auch unbefugten Clients zugänglich gemacht werden könnten, da der Benutzername und das Kennwort, die vom Web-Administrator (auf der Eigenschaftenregisterkarte Verzeichnisse des Internet-Dienst-Managers) vergeben wurden, für jeden Zugriff auf dieses freigegebene Remote-Verzeichnis verwendet werden.

Wenn man die Administration des Microsoft Index Servers über das Web durchführt, sollte man den administrativen Zugriff unbedingt streng kontrollieren. Alle administrativen Operationen auf dem Index Server werden durch die Zugriffskontrolliste (ACL) in folgendem Registrierungsschlüssel geregelt:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ContentIndex

Wenn zusätzliche Kontrollen auf administrative Operationen angewendet werden sollen, können ACLs auf die .ida-, .idq- und .htx-Dateien gelegt werden, über die der Standort verwaltet wird. Wird der Standort nur lokal statt von einem Remote-Computer aus verwaltet, können die Formulare der Administration in nur lokal zugänglichen Verzeichnissen gespeichert werden, auf die über die URL ‚file://...' zugegriffen werden kann.

Um den Standort lokal zu verwalten, müssen die Skripten auf dem Web Server in einem virtuellen Stammverzeichnis mit der Berechtigung zur Ausführung verfügbar gemacht werden.

2.8 Andere Komponenten

Da die folgenden Komponenten und ihre sicherheitsrelevanten Einstellungen abhängig von den in den vorangegangenen Kapiteln erläuterten Produkten sind und sie zudem eher selten zum Einsatz kommen dürften, wird auf eine detaillierte Beschreibung ihrer Funktionen und Sicherheitsparameter verzichtet. Sie werden nur der Vollständigkeit mit aufgeführt:

2.8.1 Microsoft Site Server

Der Microsoft Site Server 2.0 dient dazu, anspruchsvolle Web-Sites im Internet oder Intranet zu erstellen, funktionell zu erweitern und zu verwalten. Er wird in zwei unterschiedlichen Versionen angeboten:

Microsoft Site Server 2.0 und Microsoft Site Server Enterprise Edition 2.0.

Die Enterprise Edition enthält zusätzliche Leistungsmerkmale, mit denen sich Web-Sites für Internet Commerce erstellen und pflegen lassen sowie erweiterte Verwaltungsfunktionalität. Der Microsoft Site Server bietet drei Grundfunktionen, die den Bedürfnissen des jeweiligen Entwicklungsstadiums innerhalb des Lebenszyklus einer Web-Site entsprechen:

Personalisierung und Funktionserweiterung, robustes Content-Management und Verwaltung bzw. Analyse der Web-Site.

Der Verkauf von Waren und Dienstleistungen über das Internet könnte auf diese Weise abgewickelt werden. Eine fundierte Analyse der Nutzungsdaten über die Server Log-Dateien kann über vorkonfigurierte oder eigene Berichtsformate vorgenommen werden, um wichtige Rückschlüsse über die Aktivitäten auf der Web-Site zu ziehen.

2.8.2 Microsoft Merchant Server

Der Microsoft Merchant Server bietet grundlegende Funktionen, die zur Einrichtung eines virtuellen Vertriebs über das Internet benötigt werden. Neben dem einfachen Entwurf von Angebotsseiten werden auch besondere Anforderungen, wie Echtzeit-Update und automatische Bestellabwicklung abgedeckt.

2.8.3 Microsoft Transaction Server

Der Microsoft Transaction Server ist ein Produkt, das die Flexibilität und die geringen Kosten einer Desktop-Lösung mit den Transaktionsverarbeitungsfähigkeiten von Großrechnern verbindet. Microsoft Transaction Server ist ein komponentenbasiertes Transaktionsverarbeitungssystem zur Entwicklung, Installation und Verwaltung von Intranet- und Internet-Server-Anwendungen. MS Transaction Server stellt ein Anwendungsprogrammiermodell sowie eine Laufzeitinfrastruktur bereit, mit denen verteilte, komponentenbasierte Anwendungen entwikkelt und eingerichtet bzw. verwaltet werden können.

Abkürzungsverzeichnis :

ACL	Access Control List
AFP	AppleTalk Filing Protocol
AIX	Unix-Derivat von IBM
ANSI	American National Standarts Institute
API	Application Programmable Interface
APPC	Advanced Program-to-Program Communications
CA	Client Access
CAPI	Cryptography API
CAST	Verschlüsselungsalgorithmus nach Carlisle Adams und Stafford Tavares
CERN	Conseil Europeén pour la Recherche Nucléaire
CGI	Common Gateway Interface
CICS	Customer Information Control System
COM	Common Object Model
CPI-C	Common Programming Interface for Communications
CTI	Computer-Telephone Integration
DB	Datenbank
DBA	Datenbankadministrator
DBMS	Database Management System
DEC	Digital Equipment Corporation
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMI	Desktop Management Interface
DMOD	Dynamic Module
DMTF	Desktop Management Task Force
DNS	Domain Name Service
DOS	Disk Operation System
DTC	Distributed Transaction Coordinator
E/A	Eingabe/Ausgabe
EPF	Encrypted Personal File
ESSL	Enhanced SSL
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GB	Gigabyte
HP	Hewlett Packard
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IBM	International Business Machines
ICP	Internet Cache Protocol
ID	Identification
IIS	Internet Information Server
IMAP4rev1	Internet Message Access Protocol, Version 4rev1
IP	Internet Protocol
IPC	Interprocess Communication
IPX	Inter-Packet Exchange
IPXODI	IPX Open Datalink Interface
IRC	Internet Relay Chat
ISAPI	Internet Serviceleistungen API
ISDN	Integrated Services Digital Network
KM	Key Management Server
LAN	Local Area Network
LAT	Local Adress Table
LDAP	Lightweight Directory Access Protocol
LUA	Konventionelle Logical Unit Application Programmierschnittstelle
MAPI	Messaging API
MIF	Management Information File
MIME	Multipurpose Internet Mail Extensions
MPR	Multi Protocol Router
MS	Microsoft
MTA	Mail Transfer Agent
NCSA	National Center for Supercomputing Applications
NDIS	Network Driver Interface Specification
NetBEUI	NETBIOS Extended User Interface
NETBIOS	Network Basic Input Output System
NIST	National Institute for Standardisation and Technology
NNTP	Network News Transfer Protocol
NT	New Technology
NTFS	New Technology File System
ODBC	Open Database Connectivity
ODS	Open Data Services
OLE	Object Linking and Embedding
OS	Operating System
PC	Personal Computer
PCM	Package Control Manager
PDC	Primary Domain Controller
POP3	Point of Presence Protokoll V.3
PROFS	Professional Office System von IBM
PWS	Peer Web Services
RAM	Random Access Memory
RAS	Remote Access Service
RC4	Verschlüsselungsstandard
RDBMS	Relationales DBMS

RDS	Remote Data Service
RPC	Remote Procedure Call
RSA	Verschlüsselungsverfahren nach Rivest, Shamir, Adleman
RTF	Rich Text Format
RUI	Request Unit Interface
SHTTP	Secure HTTP
SLI	Session Level Interface
SMB	Server Message Block
SMP	Symetrisches Multiprozessing
SMS	Systems Management Server
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture
SNAAT	SNA ? AppleTalk Protokoll
SNADS	SNA Distribution Services
SNAIP	SNA ? Internet Protocol
SNALM	SNA ? Microsoft Networking Protokoll
SNANW	SNA ? NetWare Protokoll
SNI	Siemens Nixdorf
SNMP	Simple Network Management Protocol
SPX	Sequenced Packet Exchange Protocol
SQL	Structured Query Language
SRM	Security Reference Monitor
SSL	Secure Socket Layer
STT	Secure Transaction Technology
TAPI	Telephony API
TCP	Transmission Control Protocol
TDI	Transport Driver Interface
TKG	Telekommunikationsgesetz
TSR	Terminate and Stay Resident
TTP	Trusted Third Party
UDP	User Datagram Protocol
UNC	Uniform Naming Convention
URL	Uniform Resource Locator
VB	Visual Basic
VDOLive	Video Direct Output
VPN	Virtual Private Network
WAN	Wide Area Network
WFW	Windows for Workgroups
WWW	World Wide Web
XA	eXtended Architecture

Abbildungsverzeichnis :

Abb.1: Komponenten von Microsoft BackOffice
Abb.2: Sicherheitshierarchie
Abb.3: SQL-Sicherheitsmodi
Abb.4: Hierarchie der SQL-Sicherheitseinstellungen
Abb.5: Rechtevergabe im SQL-Enterprise-Manager
Abb.6: Der SQL-Security-Manager
Abb.7: Beispiel einer SMS-Standorthierarchie
Abb.8: SMS Sicherheitsabfrage
Abb.9: SMS-Client HelpDesk-Optionen
Abb.10: Beziehungen zwischen den Komponenten des Exchange-Servers
Abb.11: Die Konfiguration von Benutzerberechtigungen im MS Exchange-Administrator
Abb.12: Einstellung der Verschlüsselungsoptionen
Abb.13: SNA Sicherheits-Architektur
Abb.14: SNA-Server Verschlüsselungsmöglichkeiten
Abb.15: SNA-Server Beispielkonfiguration
Abb.16: Typische Installation mittelgroßer Organisationen
Abb.17: Protokollierungsmöglichkeiten des Proxy Server
Abb.18: Typische Konfiguration eines Netzwerkes mit IIS
Abb.19: Authentifizierung des Web-Zugriffs
Abb.20: Der IIS hinter einem Firewall

Literatur :

MS BackOffice allgemein:
- Intranet mit BackOffice, Stephen Wynkoop, Sams, 1997
- Special Edition: Backoffice, D. Benage & G.A. Sullivan, Que, 1997, in Deutschland erhältlich über Markt &Technik Buch- und Software- Verlag GmbH
- Special Edition Using Microsoft BackOffice, D. Benage & G.A. Sullivan et al., Que, 1997, in Deutschland erhältlich über Markt &Technik Buch- und Software- Verlag GmbH

Windows NT:
- Windows NT 4 – Netzwerkadministration & BackOffice, Thomas Dapper/Carsten Dietrich/Bert Klöppel/Jürgen Rauch/Jochen Ruhland/Klaus-Dieter Schmidt/Uwe Bergmann, Hanser, 1997
- Windows NT Server Version 4 – Die technische Referenz, Microsoft Press, 1997
- Windows NT Workstation Version 4.0 – Die technische Referenz, Microsoft Press, 1997

SQL-Server:
- Microsoft SQL Server 6.5, Dusan Petkovic, Addison-Wesley Longman, 1996
- SQL Server aus der Reihe Microsoft BackOffice – Die technische Referenz (Teil 2), Microsoft Press, 1997

Systems Management Server:
- Microsoft Systems Management Server 1.x, Jochen Gebauer, Addison-Wesley, 1997
- Systems Management Server 1.2 - MCSE Rapid Review Study Guide, Michael A. Pastore, Duke Communications, 1998
- Systems Management Server aus der Reihe Microsoft BackOffice – Die technische Referenz (Teil 1), Microsoft Press, 1997
- Systems Management Server (Zusatzband) aus der Reihe Microsoft BackOffice – Die technische Referenz (Teil 2), Microsoft Press, 1997

Exchange Server:
- Exchange Server 5 – Das Kompendium, Markt &Technik Buch- und Software- Verlag GmbH, 1997
- Exchange Server 5.5 Secrets, R. Guaraldi/J. Sides/N. Studt/J. Condon, Franzis, 1998
- Exchange Server aus der Reihe Microsoft BackOffice – Die technische Referenz (Teil 1), Microsoft Press, 1997
- Exchange Server (Zusantzband) aus der Reihe Microsoft BackOffice – Die technische Referenz (Teil 2), Microsoft Press, 1997
- Microsoft Exchange Server 5.5, Lars Riehn & Holger Kattner, Addison-Wesley Longman, 2. Auflage 1998
- MCSE Training Guide Exchange Server 5, Bruce Hallberg et al., New Riders Publishing, 1998

SNA Server:
- SNA Server aus der Reihe Microsoft BackOffice – Die technische Referenz (Teil 2), Microsoft Press, 1997

Proxy Server:
- Microsoft Internet Information Server und Microsoft Proxy Server, Microsoft Press, 1998

Internet Information Server:
- Internet Information Server 4 - The Complete Reference, John Paul Mueller & Tom Sheldon, Osborne McGrawHill, 1998
- Microsoft Internet Information Server und Microsoft Proxy Server, Microsoft Press, 1998